CARLOS DIEGO RUSSO MEDEIROS
http://www.expresso.com.br/carlos/
carlos@expresso.com.br

SEGURANÇA DA INFORMAÇÃO

Implantação de Medidas e Ferramentas de Segurança da Informação

Trabalho de Conclusão de Estágio apresentado ao Curso de Informática da Universidade da Região de Joinville – UNIVILLE – como requisito parcial para obtenção de Grau em Informática.

Orientador: Claudio Cesar de Sá

JOINVILLE
2001

RESUMO

A evolução da Internet tem facilitado extraordinariamente a comunicação entre empresas e pessoas no mundo inteiro, entretanto uma grande preocupação começou a ressurgir nesse ambiente: A Segurança da Informação. Esse é um dos assuntos mais comentados nos meios de tecnologia da informação atualmente, e com ciência da sua importância, foi proposto como projeto a ser desenvolvido no estágio supervisionado, a implantação de ferramentas e medidas para a melhoria da segurança no ambiente computacional de uma empresa. Ao longo do relatório serão apresentados os conceitos tecnológicos envolvidos neste processo, as principais técnicas de ataque e ameaças existentes, as vulnerabilidades encontradas na empresa, e os procedimentos que compuseram as aplicações práticas desse projeto. O trabalho não aspira apresentar-se como uma solução definitiva para os problemas de segurança encontrados nas organizações, mas sim, espera mostrar como aplicação correta de técnicas e ferramentas podem trazer benefícios para a segurança do ambiente computacional de uma empresa.

TERMO DE APROVAÇÃO

O aluno Carlos Diego Russo Medeiros regularmente matriculado na 4ª série do Curso de Bacharelado em Informática, apresentou e defendeu o presente Trabalho de Conclusão de Estágio, obtendo da Banca Examinadora a média final __________ (______________________________), tendo sido considerado aprovado.

Joinville, ______ de _________________ de 2001.

____

Professor

____

Professor

____

Orientador de Estágio

ÍNDICE

LISTA DE FIGURAS E TABELAS

CAPÍTULO 1 – INTRODUÇÃO

Antes da era da Internet e do comércio eletrônico, muitas vezes a informática tinha pouca importância no negócio real das empresas. A tecnologia da informação atuava na retaguarda ou na melhoria de processos, mas muito dificilmente era um elemento de negócios.

Hoje as empresas dependem cada vez mais da tecnologia da informação para o seu funcionamento, ela automatiza e ao mesmo tempo agrega valores aos processos organizacionais. Já a Internet facilita a comunicação entre empresas, funcionários, cidadãos do mundo inteiro. A grande rede está cada vez mais sendo utilizada de forma comercial, o comércio eletrônico já chega a ser considerado como marco para uma “nova economia”.

Mas com toda essa evolução começaram a surgir os problemas. A facilidade de comunicação tornou as empresas mais vulneráveis, o ambiente passou a ser heterogêneo e distribuído, difícil de ser controlado. Os ataques e invasões acontecem a todo instante, as suas conseqüências cobrem uma enorme gama de possibilidades: perda de tempo recuperando a situação anterior, queda de produtividade, perda significativa de dinheiro, horas de trabalho, devastação de credibilidade ou oportunidades de marketing, um negócio não habilitado para competir, etc. O termo Hacker, que há cinco anos atrás era praticamente desconhecido, atualmente é assunto em qualquer roda de conversas.

Em função de todos esses problemas, e da necessidade de se garantir um nível maior de segurança para o comércio eletrônico, é que as atividades do estágio foram desenvolvidas. Adequando a estrutura de tecnologia da empresa para dar sustentação ao comércio eletrônico, garantindo a segurança tanto das transações efetuadas como da própria organização; eliminando vulnerabilidades e ao mesmo tempo criando um ambiente que possa ser mais facilmente controlado e monitorado.

1.1. Identificação do Campo de Estágio

O estágio foi desenvolvido na empresa XXXXX XXXX Provedor de Acesso e Informações Ltda, uma prestadora de serviços relacionados à Internet.

Fundada em 1996, a empresa se destaca no provimento de acesso à Internet na cidade de Joinville, e nos seus serviços dedicados à tecnologia de redes de informação. Sua principal missão é prover produtos e serviços que propiciem a disseminação da informação ao longo do ambiente corporativo e residencial. Para atingir esse objetivo, utiliza como premissa o conceito de Internet Solution Provider (Provedor de Soluções Internet), e sua estratégia está focada em 5 alvos principais:

- Provimento de Acesso às redes WAN e Internet
- Consultoria e Prestação de Serviços de Segurança das Informações
- Desenvolvimento WEB e de Soluções de Comércio Eletrônico
- Integração de Sistemas à Internet
- Assessoria e Suporte Técnico especializado em Internet

As atividades de estágio foram desenvolvidas junto aos setores de administração de sistemas, segurança e desenvolvimento WEB. Mesmo assim, por se tratar de um trabalho em segurança da informação, houve a interação com todos os setores da empresa.

1.1.1. O Projeto Desenvolvido

O trabalho foi desenvolvido dentro da área de segurança da informação, envolvendo outras áreas como programação, redes e sistemas operacionais.

O escopo das atividades é a elaboração e execução de um projeto interno para aumentar o nível de segurança dos servidores de Internet da empresa. Baseado na necessidade de dar suporte aos novos serviços lançados pela empresa, especificamente no seu sistema de comércio eletrônico.

Na sua execução foram utilizadas ferramentas baseadas no sistema operacional LINUX, no qual está estruturada toda a base de servidores da empresa. Além disso, seguindo as recomendações da própria empresa, foi dada a preferência aos programas do tipo Open Source e Freeware.

Com a execução das atividades previstas no estágio pretende-se atingir os seguintes objetivos:

- Analisar e eliminar as vulnerabilidades existentes na estrutura atual
- Verificar a segurança no código programado do sistema de comércio eletrônico
- Proteger as transações e informações armazenadas no sistema.
- Desenvolver um plano de resposta a incidentes
- Proteger os servidores contra ataques

Por razões de sigilo empresarial, algumas poucas informações técnicas sobre as ferramentas e técnicas aplicadas serão omitidas ao longo desse relatório.

1.1.2. Justificativa

Devido às grandes mudanças no modelo de mercado de acesso à Internet no Brasil e no mundo, a empresa se viu obrigada a acelerar o processo de desenvolvimento de novos produtos e serviços além do acesso discado à Internet. O surgimento dos provedores de acesso gratuito, e o aumento da participação das empresas de telecomunicações diretamente no fornecimento de acesso ao consumidor final, são os principais catalisadores desse processo.

Uma das maiores apostas da Empresa é no seu sistema com comércio eletrônico (LVE – Loja Virtual XXXXX), segmento Business to Consumer (B2C - Empresa ao consumidor final), que busca disponibilizar a criação e o gerenciamento de lojas virtuais através da Internet.

Os fatores básicos para um sistema de comércio eletrônico, além da sua completa funcionalidade, são a integridade e segurança das informações trafegadas e que são utilizadas através desse sistema. Sem isso, dificilmente um projeto de comércio eletrônico obterá sucesso, pois sem a confiança e segurança dos usuários, ou melhor, compradores, as transações não se realizarão e a empresa não conseguirá alcançar os objetivos mais comuns de um projeto de comércio eletrônico: criar um novo canal de vendas de alcance mundial, melhorar o seu relacionamento com o cliente, aumentar o lucro e a competitividade.

A criação desse serviço tornou necessária a implementação de novas medidas e ferramentas de segurança que forneçam suporte ao processo de comércio eletrônico, e que ao mesmo tempo aumentem o nível de segurança da empresa como um todo. Não adianta assegurar apenas um servidor ou sistema, a segurança é como uma corrente formada por vários elos, onde a força da corrente é medida pela resistência do seu elo mais frágil.

1.1.3. Metodologia e Cronograma

Para o desenvolvimento de uma atividade em uma área tão complexa como a segurança da informação, que envolve diversas áreas da tecnologia da informação, deve haver um grande equilíbrio entre a fundamentação teórica e a experiência prática. Na busca dessa harmonia foram utilizados os seguintes métodos de trabalho:

- Revisão e aprofundamento de conhecimentos adquiridos ao longo da vida profissional e acadêmica através de pesquisas bibliográficas em livros e revistas;
- Pesquisas em sites especializados em segurança da informação;
- Estudos das ameaças e técnicas de ataque através de sites com informações utilizadas pelos atacantes (hackers);
- Experimentação prática das ferramentas envolvidas;

Outro item importante no planejamento das atividades é a alocação de tempo em cada uma das etapas do projeto. Embora a contagem de tempo esteja baseada no Plano de Estágio, algumas alterações relevantes foram realizadas antes do início do estágio.

Atividade	Previsto	Realizado
Pesquisa sobre segurança da Informação	42 H	42 H
Estudo das Técnicas de Ataque e Ameaças	42 H	42 H
Levantamento da estrutura atual da Empresa e Análise de Vulnerabilidades	32 H	32 H
Escolha e testes das ferramentas	48 H	48 H
Experimentação e Implantação das Ferramentas e Medidas de Segurança	100 H	140 H
Ajustes Finais e Correções	24 H	24 H
Cargas Horárias Totais	**288 H**	**328 H**

Tabela 1 – Cronograma das Atividades

De forma geral, o cronograma previsto foi cumprido. As distorções mais expressivas ocorreram na etapa de Implantação das ferramentas. A segmentação da rede e a aplicação de um firewall para controle do tráfego, descritas nos tópicos 3.4.1 e 3.4.2, foram as principais causadoras da extensão do tempo além do previsto.

CAPÍTULO 2 – CONCEITOS E FUNDAMENTOS

Envolvendo qualquer atividade desenvolvida na área de Tecnologia da Informação estarão sempre presentes importantes conceitos e fundamentos. Portanto é necessário apresentar os aspectos teóricos relacionados à função desempenhada no campo de estágio, evolvendo as tecnologias, ferramentas e métodos empregados na solução dos problemas observados.

É importante destacar que serão apresentados os conceitos e fundamentos pertinentes e relevantes às atividades desenvolvidas no estágio, não se esperando que o escopo e aprofundamento adotados esgotem por si só os temas abordados.

A seguir serão apresentados os principais conceitos sobre segurança da informação, envolvendo desde as principais técnicas utilizadas pelos invasores, até as principais formas de proteção.

2.1. Princípios da Segurança da Informação

A segurança da informação busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo ou organização.

Segundo PUTTINI (2001:web), uma solução de segurança adequada deve satisfazer os seguinte princípios:

- Confiabilidade: significa proteger informações contra sua revelação para alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos.
- Autenticidade: O controle de autenticidade está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema. Ela é a medida de proteção de um serviço/informação contra a personificação por intrusos.
- Integridade: A integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos ou fitas de backup. Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é assegurada evitando-se alteração não detectada de mensagens (ex. tráfego bancário) e o forjamento não detectado de mensagem (aliado à violação de autenticidade).

- Disponibilidade: consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

Através da correta aplicação desses princípios, a segurança da informação pode trazer benefícios como: aumentar a produtividade dos usuários através de um ambiente mais organizado, maior controle sobre os recursos de informática e, finalmente garantir a funcionalidade das aplicações críticas da empresa.

2.2. Criptografia

A criptografia vem, na sua origem, da fusão de duas palavras gregas:

- CRIPTO = ocultar, esconder
- GRAFIA = escrever

Criptografia é arte ou ciência de escrever em cifra ou em códigos. É então um conjunto de técnicas que tornam uma mensagem incompreensível permitindo apenas que o destinatário que conheça a chave de encriptação possa decriptar e ler a mensagem com clareza.

2.2.1. Algoritmos Criptográficos

São funções matemáticas usadas para codificar os dados, garantindo segredo e autenticação. Os algoritmos devem ser conhecidos e testados, a segurança deve basear-se totalmente na chave secreta, sendo que essa chave deve ter um tamanho suficiente para evitar sua descoberta por força-bruta[1].

Segundo PANETTA (2000:13), os algoritmos de criptografia restritos se baseiam em manter o funcionamento do algoritmo em segredo em vez de se utilizar uma chave secreta. Estes algoritmos são muito falhos porque se forem utilizados por um número grande de pessoas, a probabilidade de o seu conteúdo ser divulgado é enorme, acabando-se com o sigilo.

[1] Força-Bruta é um tipo de ataque aplicado as senhas que será descrito posteriormente no capítulo 2.3.4

De acordo com o a forma de utilização das chaves de criptografia, os algoritmos podem ser divididos em dois tipos principais: Algoritmos Simétricos e Algoritmos Assimétricos.

2.2.2. Esquemas Criptográficos Simétricos

Também denominado algoritmo simétrico, criptografia de chave simétrica ou criptografia convencional, é um sistema que utiliza apenas uma chave para encriptar e decriptar a informação.
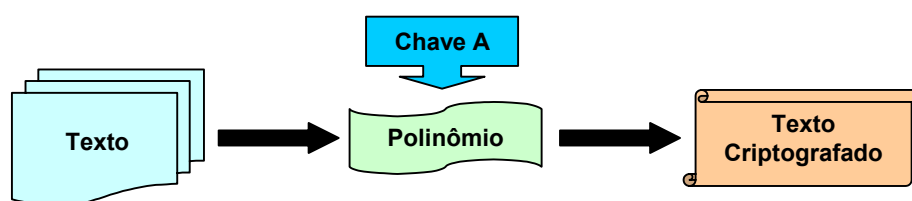
Figura 1 – Criptografia Simétrica – Encriptar
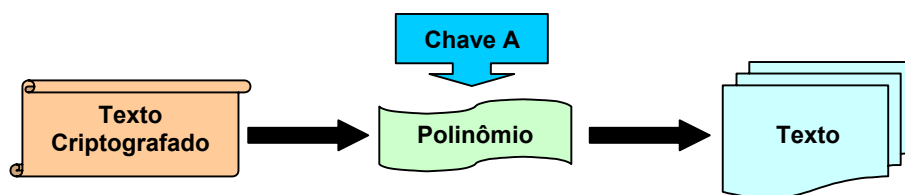
Figura 2 – Criptografia Simétrica – Decriptar

Nas figuras acima, podemos observar o funcionamento da criptografia simétrica. Uma informação é encriptada através de um polinômio utilizando-se de uma chave (Chave A) que também serve para decriptar novamente a informação.

Segundo PANETTA (2000:14) as principais vantagens dos algoritmos simétricos são:

- Rapidez: Um polinômio simétrico encripta um texto longo em milésimos de segundos
- Chaves pequenas: uma chave de criptografia de 128bits torna um algoritmo simétrico praticamente impossível de ser quebrado.

A maior desvantagem da criptografia simétrica é que a chave utilizada para encriptar é igual à chave que decripta. Quando um grande número de pessoas tem conhecimento da chave, a informação deixa de ser um segredo.

De acordo com a ED. CONSULTORIA (2001:web), os algoritmos de chave simétrica mais conhecidos são:

- DES (Data Encryption Standard): adotado pelo governo do EUA desde 1977, é um dos mais conhecidos algoritmos de criptografia e usa uma chave de 56 bits.

- DESX: é uma modificação simples do algoritmo DES em que se estabelece uma dupla criptografia.
- Triple-DES: é uma outra modificação em que se aplica três vezes o algoritmo DES com três chaves diferentes. Vem sendo usado atualmente por instituições financeiras.
- Blowfish: é um algoritmo rápido, compacto e simples, de domínio público, capaz de usar chaves de tamanho variável até 448 bits.
- IDEA (International Data Encryption Algorithm): usa chave de 128 bits e foi publicado em 1990 em Zurique na Suíça. É a base do algoritmo PGP usado em criptografia de correio eletrônico.
- O RC2 foi mantido em segredo pela RSA Data Security, até ser revelado em 1996 por uma mensagem anônima. Permite a utilização de chaves de 1 até 2048 bits.
- O RC4, também mantido em segredo pela RSA, foi revelado em 1994 e possui chave de criptografia de 1 até 2048 bits.
- O RC5 é um algoritmo publicado em 1994 que permite que o usuário escolha o tamanho da chave, o tamanho do bloco a ser criptografado e o número de vezes que o dado vai ser criptografado.

2.2.3. Esquemas Criptográficos Assimétricos

Também conhecido como algoritmo assimétrico, ou criptografia de chave-pública, é um sistema que utiliza duas chaves diferentes, uma chave denominada secreta e outra denominada pública. O par de chaves pertence a uma entidade ou pessoa e é calculado a partir de um número aleatório. O processo de criação das chaves pode ser observado na figura abaixo:
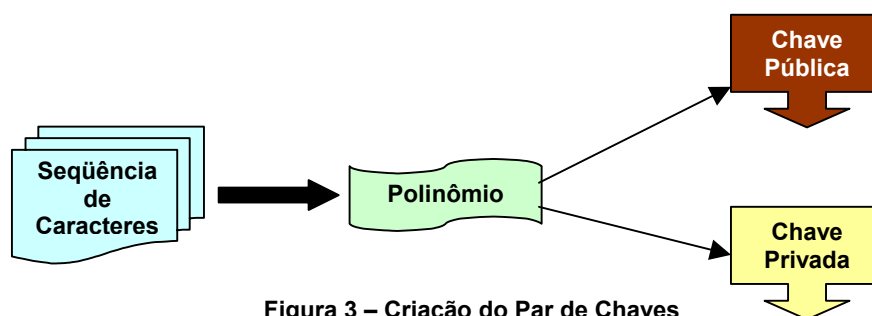
Figura 3 – Criação do Par de Chaves

A chave secreta deve ficar de posse e uso apenas de seu dono, enquanto a chave pública pode ser distribuída, inclusive para servidores específicos na Internet.

De posse da chave pública podemos criptografar informações que só poderão ser decriptadas pelo proprietário da chave privada, num processo unidirecional como pode ser observado na figura abaixo:
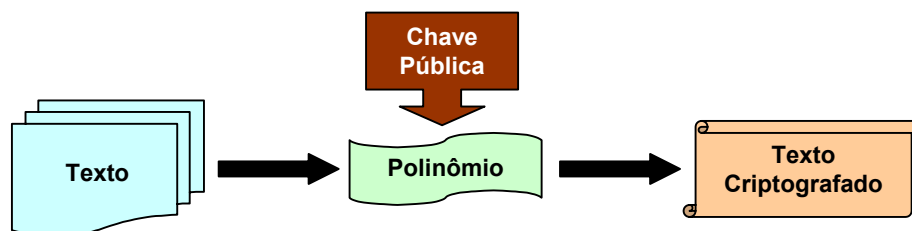
Figura 4 – Criptografia Assimétrica – Encriptar
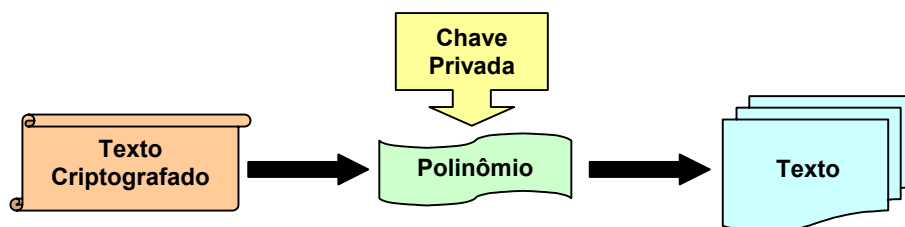
Figura 5 – Criptografia Assimétrica – Decriptar

Além disso, podemos utilizar esse mesmo recurso em sentido inverso, utilizando-se da chave-privada para criptografar uma informação que poderia ser aberta por todos que tenham posse da chave-pública desse par. Esse recurso pode parecer estranho, mas é utilizado na assinatura digital que será definida posteriormente.

Segundo PANETTA (2000:15), podemos considerar algumas desvantagens no uso de algoritmos assimétricos:

- São lentos: Um polinômio assimétrico leva mais tempo para encriptar uma informação do que um simétrico.
- Utilizam chaves grandes: uma chave de criptografia de 3078 bits torna um polinômio assimétrico equivalente a um polinômio simétrico com chave de 128 bits.

A grande vantagem do uso de criptografia assimétrica é que a chave que encripta é diferente da que decripta, garantindo uma segurança muito maior no processo.

De acordo com a ED. CONSULTORIA (2001:web), os algoritmos mais conhecidos de chave pública são:

- Diffie-Hellman: São os inventores, paralelamente com Robert Merkle, do sistema de chave pública e privada.
- RSA: Desenvolvido originalmente por Rivest, Shamir e Adleman (daí RSA), quando eram professores do MIT (Massachusets Institute of Technology), pode

ser usado tanto para criptografar informações quanto para servir de base para um sistema de assinatura digital.

- ElGamal: é basado no sistema Diffie-Hellman e pode ser usado para assinatura digital como o RSA.
- DSS (Digital Signature Standard): é usado para realização de assinatura digital, mas pode ser usado para criptografia. Atualmente usa chaves entre 512 a 1024 bits.

2.2.4. Assinatura Digital

A assinatura digital busca resolver dois problemas não garantidos apenas com uso da criptografia para codificar as informações: a Integridade e a Procedência.

Ela utiliza uma função chamada one-way hash function, também conhecida como: compression function, cryptographic checksum, message digest ou fingerprint. Essa função gera uma string única sobre uma informação, se esse valor for o mesmo tanto no remetente quanto destinatário, significa que essa informação não foi alterada.

Mesmo assim isso ainda não garante total integridade, pois a informação pode ter sido alterada no seu envio e um novo hash pode ter sido calculado.

Para solucionar esse problema, é utilizada a criptografia assimétrica com a função das chaves num sentido inverso, onde o hash é criptografado usando a chave privada do remetente, sendo assim o destinatário de posse da chave pública do remetente poderá decriptar o hash. Dessa maneira garantimos a procedência, pois somente o remetente possui a chave privada para codificar o hash que será aberto pela sua chave pública. Já o hash, gerado a partir da informação original, protegido pela criptografia, garantirá a integridade da informação.

2.2.5. Certificados Digitais

O Certificado Digital, também conhecido como Certificado de Identidade Digital, associa a identidade de um titular a um par de chaves eletrônicas (uma pública e outra privada) que, usadas em conjunto, fornecem a comprovação da identidade. É uma versão eletrônica (digital) de algo parecido a uma Cédula de Identidade - serve como prova de identidade, reconhecida diante de qualquer situação onde seja necessária a comprovação de identidade.

O Certificado Digital pode ser usado em uma grande variedade de aplicações, como comércio eletrônico, groupware (Intranet's e Internet) e transferência eletrônica de fundos.

Dessa forma, um cliente que compre em um shopping virtual, utilizando um Servidor Seguro, solicitará o Certificado de Identidade Digital deste Servidor para verificar: a identidade do vendedor e o conteúdo do Certificado por ele apresentado. Da mesma forma, o servidor poderá solicitar ao comprador seu Certificado de Identidade Digital, para identificá-lo com segurança e precisão.

Caso qualquer um dos dois apresente um Certificado de Identidade Digital adulterado, ele será avisado do fato, e a comunicação com segurança não será estabelecida.

O Certificado de Identidade Digital é emitido e assinado por uma Autoridade Certificadora Digital (Certificate Authority). Para tanto, esta autoridade usa as mais avançadas técnicas de criptografia disponíveis e de padrões internacionais (norma **ISO X.509 para Certificados Digitais**), para a emissão e chancela digital dos Certificados de Identidade Digital.

PANETTA (2001:13) descreve os elementos de certificado digital, sendo que podemos destacar os três elementos principais:

Informação de atributo: É a informação sobre o objeto que é certificado. No caso de uma pessoa, isto pode incluir seu nome, nacionalidade e endereço e-mail, sua organização e o departamento da organização onde trabalha.

Chave de informação pública: É a chave pública da entidade certificada. O certificado atua para associar a chave pública à informação de atributo, descrita acima. A chave pública pode ser qualquer chave assimétrica, mas usualmente é uma chave RSA.

Assinatura da Autoridade em Certificação (CA) : A CA assina os dois primeiros elementos e, então, adiciona credibilidade ao certificado. Quem recebe o certificado verifica a assinatura e acreditará na informação de atributo e chave pública associadas se acreditar na Autoridade em Certificação.

Existem diversos protocolos que usam os certificados digitais para comunicações seguras na Internet:

- Secure Socket Layer ou SSL
- Secured Multipurpose Mail Extensions - S/MIME
- Form Signing
- Authenticode / Objectsigning

O SSL é talvez a mais difundida aplicação para os certificados digitais e é usado em praticamente todos os sites que fazem comércio eletrônico na rede (livrarias, lojas de CD, bancos etc.). O SSL teve uma primeira fase de adoção onde apenas os servidores estavam identificados com certificados digitais, e assim tínhamos garantido, além da identidade do servidor, o sigilo na sessão. Entretanto, apenas com a chegada dos certificados para os browsers é que pudemos contar também com a identificação na ponta cliente, eliminando assim a necessidade do uso de senhas e logins.

O S/Mime é também um protocolo muito popular, pois permite que as mensagens de correio eletrônico trafeguem encriptadas e/ou assinadas digitalmente. Desta forma os e-mails não podem ser lidos ou adulterados por terceiros durante o seu trânsito entre a máquina do remetente e a do destinatário. Além disso, o destinatário tem a garantia da identidade de quem enviou o e-mail.

O Form Signing é uma tecnologia que permite que os usuários emitam recibos online com seus certificados digitais. Por exemplo: o usuário acessa o seu Internet Banking e solicita uma transferência de fundos. O sistema do banco, antes de fazer a operação, pede que o usuário assine com seu certificado digital um recibo confirmando a operação. Esse recibo pode ser guardado pelo banco para servir como prova, caso o cliente posteriormente negue ter efetuado a transação.

O Authenticode e o Object Signing são tecnologias que permitem que um desenvolvedor de programas de computador assine digitalmente seu software. Assim, ao baixar um software pela Internet, o usuário tem certeza da identidade do fabricante do programa e que o software se manteve íntegro durante o processo de download. Os certificados digitais se dividem em basicamente dois formatos: os certificados de uso geral (que seriam equivalentes a uma carteira de identidade) e os de uso restrito (equivalentes a cartões de banco, carteiras de clube etc.). Os certificados de uso geral são emitidos diretamente para o usuário final, enquanto que os de uso restrito são voltados basicamente para empresas ou governo.

2.2.6. SSL – Secure Sockets Layer

O SSL é um protocolo de segurança projetado pela Netscape Communications Corporation, a empresa do famoso browser Netscape. O SSL destina-se a dar segurança durante a transmissão de dados sensíveis por TCP/IP[2].

---

[2] TCP/IP é o protocolo de comunicação utilizado na Internet. Devido a sua grande aceitação ele acabou se tornando também o protocolo padrão para redes locais

O SSL fornece criptografia de dados, autenticação de servidor e integridade de mensagem para transmissão de dados pela Internet. O SSL versão 2.0 suporta apenas autenticação de servidor, ao passo que a versão 3.0 suporta a autenticação tanto de cliente como de servidor.

Quando o browser ("cliente") conecta-se a uma página protegida por SSL, o servidor do SSL envia uma solicitação para iniciar a sessão segura. Se o browser suporta SSL, ele retorna uma resposta. Durante este handshake ("apertar de mãos") inicial, o servidor e o browser trocam informações seguras. A resposta do browser define um número único para identificar para sessão, os algoritmos de criptografia e os métodos de compactação que suporta. Nas informações de segurança fornecidas pelo browser, o servidor faz sua seleção e a comunica ao browser. O servidor e o browser, em seguida, trocam certificados digitais. O servidor também especifica uma chave pública ("chave de sessão") apropriada para o algoritmo de criptografia anteriormente selecionado. O browser pode, então, usar a chave pública para criptografar informações enviadas ao servidor, sendo que o servidor pode usar sua chave privada para descriptografar essas mensagens. Depois que o servidor e o browser estão de acordo sobre a organização da segurança, as informações podem ser transmitidas entre os dois, em um modo seguro.

Os dados protegidos pelo protocolo envolvem o uso de criptografia e decriptografia, portanto, o uso do SSL envolve uma carga extra. De fato, o seu uso não apenas aumenta a quantidade de dados transmitidos, mas também cria mais pacotes, tornando mais lenta a transmissão de informações entre o servidor e o browser.

Entretanto, ele pode ser implementado no nível da página da Web. Ou seja, não é necessário implementar proteção do protocolo para cada página de um site na Web que forneça proteção de SSL. O método mais comum da sua implementação para aplicações de comércio eletrônico é proteger com o SSL apenas aquelas páginas que contêm informações confidenciais e sensíveis, tais como informações pessoais e de cartão de crédito.

A maioria dos browsers que suporta o protocolo fornece alguma indicação de que uma determinada página da Web está protegida. Por exemplo, o Netscape Navigator indica se uma página da Web tem proteção SSL ao exibir um ícone de segurança em forma de chave, no canto inferior esquerdo da janela do browser. No Netscape Communicator, é exibido um cadeado fechado na mesma posição. No Internet Explorer 3.0 e 4.0, o SSL é indicado com a exibição de um cadeado no canto inferior direito da janela do browser.

Atualmente o mecanismo de criptografia do SSL utiliza chave pública RSA com chaves de 128bits para implementar transmissão segura. Quanto maior o número de bits na chave criptografia, tanto mais difícil será quebrar a chave.

2.2.7. SET - Secure Electronic Transaction

O SET é um protocolo aberto para transmissão segura de informações de pagamento pela Internet ou outras redes eletrônicas.

O processo envolve várias verificações de segurança usando certificados digitais, os quais são emitidos aos compradores participantes, comerciantes e instituições financeiras.

O SET utiliza combinações de criptografia DES e RSA. Chaves públicas e privadas são utilizadas por todos os participantes da transação. Os certificados são emitidos pela organização padronizadora do protocolo, chamada SETCo, que inclui a VISA e MASTERCARD.

De acordo com a SETCo (2001:web), podemos definir alguns componentes que fazem parte do protocolo:

- Cardholder Application: Também conhecido como carteira eletrônica, é uma aplicação utilizada pelo consumidor que permite o pagamento seguro através da rede. As aplicações de carteiras eletrônicas devem gerar mensagens no protocolo SET que possam ser aceitas pelos componentes SET Merchant, Payment Gateway e Cerficate Authority.
- Merchant Server component: é um produto utilizado pelo comerciante on-line para processar e autorizar os pagamentos por cartão. Ele se comunica com os componentes Cardholder Application, Payment Gateway e Certificate Authority.
- Payment Gateway: é utilizado por organizações que processam as mensagens de autorização e pagamento, emitidas pelo Merchant Server, com as redes das instituições financeiras.
- Certificate Authority: é o componente utilizado pelas instituições financeiras ou terceiros previamente aprovados para emitir certificados digitais requeridos por todos os outros componentes.

A maior vantagem do padrão SET é a utilização de certificados digitais que garantem a segurança da transação tanto do lado do consumidor, que recebe um certificado do comerciante, quanto do lado do comerciante, que tem a certeza de estar realizando um negócio com um cliente também certificado. Os certificados digitais reforçam as relações de confiança e fornecem uma maior proteção contra fraudes, a qual não é encontrada nos sistemas atuais. Além disso, com a utilização do SET o comerciante não tem acesso aos dados de cartão de crédito do cliente, visto que os dados são enviados diretamente para operadora de cartão que aprova o pagamento e transfere os fundos para o comerciante. Dessa forma é possível garantir que os dados sigilosos da compra não estarão vulneráveis a falhas de segurança nos servidores da loja virtual.

Mesmo com essas vantagens, um problema surge com a sua utilização. O padrão especifica que os consumidores também devem ter seus próprios certificados, e ainda devem possuir a sua carteira eletrônica. Esse processo de certificação e instalação da carteira envolve a interação do consumidor, que nem sempre é aceita de maneira direta, pois apesar das vantagens, essa é uma tecnologia um tanto que complexa. Esses fatores acabam prejudicando a ascensão desse protocolo.

2.2.8. VPNs - Virtual Private Network

Conforme o conceito apresentado no Guia de Conectividade CYCLADES (1999:98), Virtual Private Network (VPN) ou Rede Virtual Privada é uma rede privada (rede com acesso restrito) construída sobre a estrutura de uma rede pública (recurso público, sem controle sobre o acesso aos dados), normalmente a Internet. Ou seja, ao invés de se utilizar links dedicados ou redes de pacotes para conectar redes remotas, utiliza-se a infra-estrutura da Internet, uma vez que para os usuários a forma como as redes estão conectadas é transparente.

Normalmente as VPNs são utilizadas para interligar empresas onde os custos de linhas de comunicação direta de dados são elevados.

Elas criam túneis virtuais de transmissão de dados utilizando criptografia para garantir a privacidade e integridade dos dados, e a autenticação para garantir que os dados estão sendo transmitidos por entidades ou dispositivos autorizados e não por outros quaisquer.

Uma VPN pode ser implementada tanto por dispositivos específicos, softwares ou até pelo próprio sistema operacional.

Alguns aspectos negativos também devem ser considerados sobre a utilização de VPNs:

- Perda de velocidade de transmissão: as informações criptografadas têm seu tamanho aumentado, causando uma carga adicional na rede.
- Maiores exigências de processamento: o processo de criptografar e decriptar as informações transmitidas gera um maior consumo de processamento entre os dispositivos envolvidos.

2.2.9. Considerações sobre Criptografia

Muitas vezes a criptografia é considerada como sinônimo de segurança. A criptografia é necessária, mas não suficiente, para uma segurança forte. Na Internet, a maioria das criptografias é utilizada em aplicações como e-mail e softwares de navegação. Contudo, ataques comuns aos sistemas operacionais podem superar as aplicações de criptografia e mesmo a autenticação de sistema operacional. O uso de criptografia isoladamente não aumenta a resistência à invasão de sistemas. Por isso, outras técnicas serão apresentadas adiante na seção 2.4, que servem como instrumento para aumentar a segurança.

2.3. Técnicas de Ataque e Ameaças

Para se garantir a proteção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataque utilizadas pelos invasores, para então aplicar as medidas e ferramentas necessárias para proteção desses recursos.

Sem o conhecimento desses fatores, toda a aplicação de mecanismos de proteção pode ser anulada, pois se existir algum ponto vulnerável ou protegido de maneira incorreta, todo sistema estará comprometido.

Dessa maneira, esta seção busca identificar as principais ameaças e técnicas de ataque contra a segurança da informação.

2.3.1. Sniffers – Farejadores

"Por padrão, os computadores (pertencentes à mesma rede) escutam e respondem somente pacotes endereçados a eles. Entretanto, é possível utilizar um software que coloca a interface num estado chamado de modo promíscuo. Nessa condição o computador pode monitorar e capturar os dados trafegados através da rede, não importando o seu destino legítimo." (ANONYMOUS, 1999:194)

Os programas responsáveis por capturar os pacotes de rede são chamados Sniffers, Farejadores ou ainda Capturadores de Pacote. Eles exploram o fato do tráfego dos pacotes das aplicações TCP/IP não utilizar nenhum tipo de cifragem nos dados. Dessa maneira um sniffer pode obter nomes de usuários, senhas ou qualquer outra informação transmitida que não esteja criptografada.

A dificuldade no uso de um sniffer é que o atacante precisa instalar o programa em algum ponto estratégico da rede, como entre duas máquinas, (com o tráfego entre elas passando pela máquina com o farejador) ou em uma rede local com a interface de rede em modo promíscuo.

2.3.2. Spoofing – Falsificação de Endereço

ANONYMOUS (1999:272) define spoofing como sendo uma técnica utilizada por invasores para conseguirem se autenticar a serviços, ou outras máquinas, falsificando o seu endereço de origem. Ou seja, é uma técnica de ataque contra a autenticidade, uma forma de personificação que consiste em um usuário externo assumir a identidade de um usuário ou computador interno, atuando no seu lugar legítimo.

A técnica de spoofing pode ser utilizada para acessar serviços que são controlados apenas pelo endereço de rede de origem da entidade que irá acessar o recurso específico, como também para evitar que o endereço real de um atacante seja reconhecido durante uma tentativa da invasão.

Essa técnica é utilizada constantemente pelos Hackers, sendo que existem várias ferramentas que facilitam o processo de geração de pacotes de rede com endereços falsos.

2.3.3. DoS - Denial-of-Service

Ter as informações acessíveis e prontas para uso representa um objetivo crítico para muitas empresas. No entanto, existem ataques de negação de serviços (DoS – Denial-of-Service Attack), onde o acesso a um sistema/aplicação é interrompido ou impedido, deixando de estar disponível; ou uma aplicação, cujo tempo de execução é crítico, é atrasada ou abortada.

Esse tipo de ataque é um dos mais fáceis de implementar e mais difíceis de se evitar. Geralmente usam spoofing para esconder o endereço de origem do ataque. O objetivo é incapacitar um servidor, uma estação ou algum sistema de fornecer os seus serviços para os usuários legítimos. Normalmente o ataque DoS não permite o acesso ou modificação de dados. Usualmente o atacante somente quer inabilitar o uso de um serviço, não corrompê-lo.

De acordo com LIMA (2000:16), podemos destacar algumas das formas para realização de ataques de negação de serviço:

- Flooding – O atacante envia muitos pacotes de rede em curto período de tempo, de forma que a máquina vítima fique sobrecarregada e comece a descartar pacotes (negar serviços).
- Buffer Overflow – Uma máquina pode negar serviços se algum software ou sistema operacional tiver alguma falha com o processo de alocação de memória e com o limitado tamanho dos buffers usados. Existem ataques que exploram estes problemas de implementação para, inclusive, rodar código executável remotamente na máquina vítima.
- Pacotes Anormais – Algumas implementações do protocolo TCP/IP não consideram o recebimento de pacotes com formato dos seus dados de maneira incorreta, dessa maneira muitas vezes é possível até travar completamente uma máquina ou equipamento remoto enviando pacotes com dados inválidos.

Apesar de geralmente não causarem a perda ou roubo de informações, os ataques DoS são extremamente graves. Um sistema indisponível, quando um usuário autorizado necessita dele, pode resultar em perdas tão graves quanto às causadas pela remoção das informações daquele sistema. Ele ataca diretamente o conceito de disponibilidade, ou seja, significa realizar ações que visem a negação do acesso a um serviço ou informação.

2.3.4. DDoS – Distributed Denial-of-Services Attacks

Ao longo de 1999 e 2000, diversos sites sobre segurança da informação (como o CERT, SANS e SecurityFocus) começaram a anunciar uma nova categoria de ataques de rede que acabou se tornando bastante conhecida: o ataque distribuído. Neste novo enfoque, os ataques não são baseados no uso de um único computador para iniciar um ataque, no lugar são utilizados centenas ou até milhares de computadores desprotegidos e ligados na Internet para lançar coordenadamente o ataque. A tecnologia distribuída não é completamente nova, no entanto, vem amadurecendo e se sofisticando de tal forma que até mesmo vândalos curiosos e sem muito conhecimento técnico podem causar danos sérios.

Seguindo na mesma linha de raciocínio, os ataques *Distributed Denial of Service*, nada mais são do que o resultado de se conjugar os dois conceitos: negação de serviço e intrusão distribuída. Os ataques DDoS podem ser definidos como ataques DoS diferentes partindo de várias origens, disparados simultânea e coordenadamente sobre um ou mais alvos. De uma maneira simples, são ataques DoS em larga escala.

De acordo com o CERT (2000:web), os primeiros ataques DDoS documentados surgiram em agosto de 1999, no entanto, esta categoria se firmou como a mais nova

ameaça na Internet na semana de 7 a 11 de Fevereiro de 2000, quando vândalos cibernéticos deixaram inoperantes por algumas horas sites como o Yahoo, EBay, Amazon e CNN. Uma semana depois, teve-se notícia de ataques DDoS contra sites brasileiros, tais como: UOL, Globo On e IG, causando com isto uma certa apreensão generalizada.

Para realização de um ataque DDoS são envolvidos os seguintes personagens:

- **Atacante:** Quem efetivamente coordena o ataque.
- **Master:** Máquina que recebe os parâmetros para o ataque e comanda os agentes.
- **Agente:** Máquina que efetivamente concretiza o ataque DoS contra uma ou mais vítimas, conforme for especificado pelo atacante. Geralmente um grande número de máquinas que foram invadidas para ser instalado o programa cliente.
- **Vítima:** Alvo do ataque. Máquina que é "inundada" por um volume enorme de pacotes, ocasionando um extremo congestionamento da rede e resultando na paralisação dos serviços oferecidos por ela.

Vale ressaltar que, além destes, existem outros dois personagens atuando nos bastidores:

- ***Daemon**:* Processo que roda no agente, responsável por receber e executar os comandos enviados pelo cliente.
- ***Cliente**:* Aplicação que reside no *master* e que efetivamente controla os ataques enviando comandos aos daemons.

Os ataques DDoS amplificam o poder de ação dos ataques DoS utilizando computadores comprometidos, os agentes, onde os daemons foram instalados indevidamente devido a vulnerabilidades exploradas pelos atacantes. A partir do momento que o master envia o comando de início para os agentes, o ataque à vítima se inicia em grande escala. Esse tipo de ataque mostra como a segurança de qualquer equipamento à Internet é importante, qualquer host vulnerável pode ser utilizado como recurso para um ataque.

2.3.5. Ataque de Senhas

Segundo CLIFF (2001:web), a utilização de senhas seguras é um dos pontos fundamentais para uma estratégia efetiva de segurança. As senhas garantem que somente as pessoas autorizadas terão acesso a um sistema ou à rede. Infelizmente isso nem sempre é realidade. As senhas geralmente são criadas e implementadas pelos próprios usuários que utilizam os sistemas ou a rede. Palavras, símbolos ou datas fazem com que as senhas tenham algum significado para os usuários, permitindo que eles possam facilmente lembra-las. Neste ponto é que existe o problema, pois muitos usuários priorizam a conveniência ao invés da segurança. Como resultado, eles escolhem senhas que são relativamente simples. Enquanto isso permite que possam lembrar facilmente das senhas, também facilita o trabalho de quebra dessas senhas por hackers. Em virtude disso, invasores em potencial estão sempre testando as redes e sistemas em busca de falhas para entrar. O modo mais notório e fácil a ser explorado é a utilização de senhas inseguras. A primeira linha de defesa, a utilização de senhas, pode se tornar um dos pontos mais falhos.

Parte da responsabilidade dos administradores de sistemas é garantir que os usuários estejam cientes da necessidade de utilizar senhas seguras. Isto leva a dois objetivos a serem alcançados: primeiro, educar os usuários sobre a importância do uso de senhas seguras; e segundo, implementar medidas que garantam que as senhas escolhidas pelos usuários são efetivamente adequadas. Para alcançar o primeiro objetivo, a educação do usuário é o ponto chave. Já para alcançar o segundo objetivo, é necessário que o administrador de sistemas esteja um passo à frente, descobrindo senhas inseguras antes dos atacantes. Para fazer isso é necessária a utilização das mesmas ferramentas utilizadas pelos atacantes.

CLIFF (2001:web) descreve as duas principais técnicas de ataque a senhas:

- **Ataque de Dicionário:** Nesse tipo de ataque são utilizadas combinações de palavras, frases, letras, números, símbolos, ou qualquer outro tipo de combinação geralmente que possa ser utilizada na criação das senhas pelos usuários. Os programas responsáveis por realizar essa tarefa trabalham com diversas permutações e combinações sobre essas palavras. Quando alguma dessas combinações se referir à senha, ela é considerada como quebrada (Cracked). Geralmente as senhas estão armazenadas criptografadas utilizando um sistema de criptografia HASH. Dessa maneira os programas utilizam o mesmo algoritmo de criptografia para comparar as combinações com as senhas armazenadas. Em outras palavras, eles adotam a mesma configuração de criptografia das senhas, e então criptografam as palavras do dicionário e comparam com senha.

- **Força-Bruta:** Enquanto as listas de palavras, ou dicionários, dão ênfase a velocidade, o segundo método de quebra de senhas se baseia simplesmente na repetição. Força-Bruta é uma forma de se descobrir senhas que compara cada combinação e permutação possível de caracteres até achar a senha. Este é um método muito poderoso para descoberta de senhas, no entanto é extremamente lento porque cada combinação consecutiva de caracteres é comparada.
  Ex: *aaa, aab, aac ..... aaA, aaB, aaC... aa0, aa1, aa2, aa3... aba, aca, ada...*

2.3.6. Malware – Vírus, Trojans e Worms

"Vírus, Trojans, Worms. Batizadas genericamente de Malware, as pragas virtuais têm ganhado terreno nos últimos anos no que diz respeito aos prejuízos encarados por empresas. Como se defender com eficiência contra as pragas é a pergunta que povoa a mente de administradores, gestores de segurança e empresários, cada vez mais preocupados com as perdas que enfrentam ao ingressar nesse admirável mundo novo chamado Internet. Se houvesse apenas uma resposta para essa dúvida, de como aproveitar todos os recursos trazidos pela rede sem sofrer com os riscos, estariam todos satisfeitos. Mas, infelizmente, a experiência mostra que lidar com ameaças virtuais exige uma série de cuidados que não se restringe ao uso de antivírus." (HAICAL, 2001:web)

Através do gráfico abaixo, é possível conferir o avanço das pragas virtuais nos últimos anos:
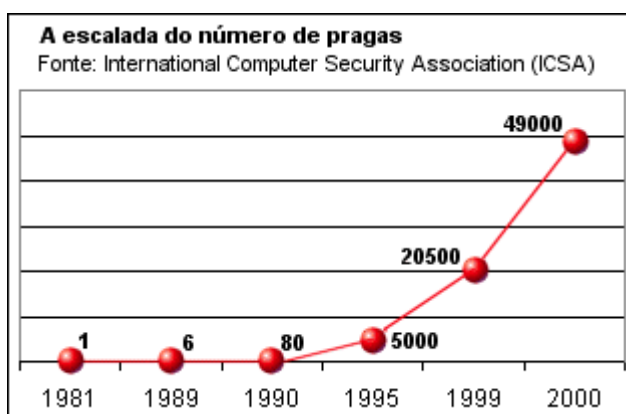
Figura 6 – Gráfico Evolução do Número de Malwares

2.3.6.1. Vírus

"Provavelmente o tipo de quebra de segurança mais conhecido popularmente é o vírus" ED. CONSULTORIA (2001:web)

Os vírus são programas espúrios inseridos em computadores contra vontade do usuário e desempenham funções indesejadas.

Alguns vírus têm a capacidade de se reproduzir e infectar outros dispositivos por toda a rede. Já outros não se reproduzem, mas são distribuídos em falsos programas na rede ou em CDs vendidos em publicações.

A cada dia surgem centenas de vírus e o combate a esse tipo de invasão é uma tarefa constante.

As principais contra-medidas são a instalação de programas antivírus atualizados em todos as estações de trabalho e servidores. É recomendável deixar programas antivírus residentes na memória para proteção em tempo real de qualquer infecção possível.

Também se deve restringir as permissões de acesso especialmente a programas executáveis, impedindo que sejam alterados. Deve-se restringir acesso a pastas e diretórios críticos especialmente em servidores.

Os usuários devem ser alertados dos riscos que correm ao instalar programas suspeitos ou não autorizados em suas estações de trabalho.

2.3.6.2. Trojans – Cavalos de Tróia

O nome foi baseado na clássica peça da mitologia grega onde os soldados do país conseguem se infiltrar na cidade de Tróia escondidos dentro de um imenso cavalo de madeira.

ANONYMOUS (1999:168) define os Cavalos-de-tróia como programas projetados para assumir controle de um servidor ou estação de trabalho de maneira furtiva, sem que o administrador de rede ou usuário se dê conta.

Para que o invasor descubra quem possui a parte servidor do software ele faz uma varredura de endereços na Internet. Quem estiver infectado pelo cavalo-de-tróia responderá à varredura.

Os Trojans são códigos maliciosos, geralmente camuflados como programas inofensivos que, uma vez instalados no computador da vítima, podem permitir que o criador da praga obtenha o controle completo sobre a máquina infectada, que passa a ser chamada de "zumbi". Os programas para ataques Denial-of-Service (DoS) geralmente são Trojans.

Alguns tipos de Trojans conhecidos, como o BO e o Netbus, permitem acesso ao computador, deixando vulneráveis arquivos do sistema e senhas gravadas no disco e na memória. Neste caso, um usuário de Internet banking infectado pela praga pode estar fornecendo sem saber o passaporte para a sua conta corrente.

Para evitar a infecção por cavalos-de-tróia, muitos sites visados pelos invasores disponibilizam arquivos para download com esquemas de verificação de integridade como verificação de soma, PGP, entre outros.

É sempre bom certificar-se da origem de programas baixados pela Internet.

2.3.6.3. Worms

São trojans ou vírus que fazem cópias do seu próprio código e as enviam para outros computadores, seja por e-mail ou via programas de bate-papo, dentre outras formas de propagação pela rede. Eles têm se tornado cada vez mais comuns e perigosos porque o seu poder de propagação é muito grande.

Do lado dos servidores, os worms mais recentes exploram vulnerabilidades dos serviços ou programas instalados no servidor para se infiltrar e fornecer acesso ao atacante. Além disso, uma vez instalados eles começam a procurar novos endereços vulneráveis para atacar.

Já do lado das estações, os worms mais comuns exploram vulnerabilidades dos programas de recebimento de e-mail para se infiltrarem e se propagarem para todas os endereços cadastrados no cliente de e-mail, além de se anexarem automaticamente em todas as mensagens enviadas.

Os worms são uma das pragas mais perigosas atualmente, eles unem o conceito de vírus e trojan utilizando a internet para se propagarem automaticamente.

2.3.7. Port Scanning

Port Scaning é o processo de verificação de quais serviços estão ativos em um determinado host. Segundo FYODOR (2001:web), as ferramentas de Port Scanning podem verificar redes inteiras, apontando quais hosts[3] estão ativos e quais são os seus serviços de rede em funcionamento. Além disso, as ferramentas mais modernas inclusive podem informar qual é o sistema operacional do host verificado.

---

[3] Hosts podem ser considerados como estações , servidores ou equipamentos ligados em rede.

Essa é geralmente a primeira técnica utilizada por hackers para se obter informações sobre o seu alvo. Sabendo quais são os serviços disponíveis e qual o sistema operacional, eles podem buscar por vulnerabilidades nesses sistemas. Para realizar um trabalho obscuro, muitas das ferramentas de Port Scanning utilizam técnicas como Spoofing para ocultar origem da sua ação. Além disso, elas também possuem um tipo de scanning chamado “Stealth”, que dificilmente pode ser detectado.

LIMA (2000:16) descreve que a técnica de Port Scanning também pode ser utilizada pelos administradores de sistemas para realizar uma auditoria nos serviços ativos da rede. Dessa maneira, pode-se identificar e eliminar quaisquer serviços que estejam rodando sem necessidade, auxiliando na manutenção da segurança.

O Port Scanning é muito útil, tanto para os administradores de sistemas quanto para os Hackers. Atualmente existem ferramentas que podem identificar e reagir contra essa técnica, elas devem ser utilizadas com precaução, pois os invasores podem estar utilizando endereços falsos, dessa maneira uma reação poderia estar sendo realizada contra o host errado.

2.3.8. Engenharia Social

Os Administradores de Sistemas e Analistas de Segurança tem a tarefa de garantir que a rede e os sistemas estejam disponíveis, operacionais e íntegros. Eles utilizam as últimas ferramentas e tecnologias disponíveis para atingir esses objetivos. Infelizmente não importa quanto dinheiro em equipamentos ou programas forem investidos na segurança, sempre haverá um elemento desprezado: O elemento humano. Muitos atacantes com conhecimentos medíocres de programação podem vencer ou ultrapassar a maioria das defesas utilizando uma técnica designada como Engenharia Social.

Segundo TIMS (2001:web), na segurança da informação a Engenharia Social é a aquisição de alguma informação ou privilégios de acesso inapropriado por alguém do lado de fora, baseado na construção de relações de confiança inapropriadas com as pessoas de dentro de uma organização. Ou seja, é a arte de manipular pessoas a fazer ações que elas normalmente não fazem. O objetivo da Engenharia Social, como técnica de ataque à segurança, é enganar alguma pessoa para que ela diretamente forneça informações, ou facilite o acesso a essas informações. Essa técnica é baseada nas qualidades da natureza humana, como a vontade de ajudar, a tendência em confiar nas pessoas e o medo de “se meter em problemas”. O resultado de uma ação de Engenharia Social bem sucedida é o fornecimento de informações ou acesso a invasores sem deixar nenhuma suspeita do que eles estão fazendo.

A Engenharia Social é um problema sério. Uma organização deve pregar uma política que possa protegê-la contra essa ameaça, sendo que essa política deve ser repassada para toda a organização. Não adianta implementar as mais modernas ferramentas de segurança se os funcionários fornecem “a chave da porta” para todos que pedirem.

2.4. Métodos e Ferramentas de Segurança

Uma vez conhecidos as principais ameaças e técnicas utilizadas contra a segurança da Informação, pode-se descrever as principais medidas e ferramentas necessárias para eliminar essas ameaças e garantir a proteção de um ambiente computacional. É nesse sentido que essa nova seção será apresentada.

2.4.1. Segurança Física

Devemos atentar para ameaças sempre presentes, mas nem sempre lembradas; incêndios, desabamentos, relâmpagos, alagamentos, problemas na rede elétrica, acesso indevido de pessoas aos servidores ou equipamentos de rede, treinamento inadequado de funcionários, etc.

Medidas de proteção física, tais como serviços de guarda, uso de no-breaks, alarmes e fechaduras, circuito interno de televisão e sistemas de escuta são realmente uma parte da segurança da informação. As medidas de proteção física são freqüentemente citadas como “segurança computacional”, visto que têm um importante papel também na prevenção dos itens citados no parágrafo acima.

O ponto-chave é que as técnicas de proteção de dados por mais sofisticadas que sejam, não têm serventia nenhuma se a segurança física não for garantida.

2.4.2. Instalação e Atualização

A maioria dos sistemas operacionais, principalmente as distribuições Linux, vem acompanhada de muitos aplicativos que são instalados opcionalmente no processo de instalação do sistema. Podemos tomar como exemplo a distribuição RedHat Linux, que na sua versão mais atual (7.1) vem acompanhada de dois CDs com mais de 3000 aplicativos. Muitas vezes a instalação desses aplicativos não focaliza a segurança, mas sim a facilidade

de uso. Sendo assim, torna-se necessário que vários pontos sejam observados para garantir a segurança desde a instalação do sistema, dos quais podemos destacar:

- **Seja minimalista:** Instale somente os aplicativos necessários, aplicativos com problemas podem facilitar o acesso de um atacante.
- **Devem ser desativados todos os serviços de sistema que não serão utilizados:** Muitas vezes o sistema inicia automaticamente diversos aplicativos que não são necessários, esses aplicativos também podem facilitar a vida de um atacante.
- **Deve-se tomar um grande cuidado com as aplicações de rede:** problemas nesse tipo de aplicação podem deixar o sistema vulnerável a ataques remotos que podem ser realizados através da rede ou Internet.
- **Use partições diferentes para os diferentes tipos de dados:** a divisão física dos dados facilita a manutenção da segurança.
- **Remova todas as contas de usuários não utilizadas:** Contas de usuários sem senha, ou com a senha original de instalação, podem ser facilmente exploradas para obter-se acesso ao sistema.

De acordo com diversos anúncios publicados pelo CERT (2000:web), grande parte das invasões na Internet acontece devido à falhas conhecidas em aplicações de rede, as quais os administradores de sistemas não foram capazes de corrigir a tempo. Essa afirmação pode ser confirmada facilmente pelo simples fato de que quando uma nova vulnerabilidade é descoberta, um grande número de ataques é realizado com sucesso. Por isso é extremamente importante que os administradores de sistemas se mantenham atualizados sobre os principais problemas encontrados nos aplicativos utilizados, através dos sites dos desenvolvedores ou específicos sobre segurança da Informação. As principais empresas comerciais desenvolvedoras de software e as principais distribuições Linux possuem boletins periódicos informando sobre as últimas vulnerabilidades encontradas e suas devidas correções. Alguns sistemas chegam até a possuir o recurso de atualização automática, facilitando ainda mais o processo.

2.4.3. Desenvolvimento Seguro de Aplicações WEB

O desenvolvimento de aplicações que irão utilizar a internet como interface, designadas aqui como Aplicações WEB, exige uma maior preocupação com a segurança no processamento e armazenamento dos dados. Esse tipo de aplicação fica exposta um grande número de usuários e ameaças. Hackers estão constantemente testando as

aplicações em busca de vulnerabilidades que possam facilitar o acesso a um sistema, ou simplesmente falhas que possam negar um serviço, como nos ataques DoS ou DDoS.

Sendo assim, podemos destacar algumas das principais práticas para o desenvolvimento seguro de aplicações WEB descritas por PETEANU (2000:web):

- Não use mais poder do que o necessário: As aplicações devem rodar num nível de acesso suficiente para utilizar somente os recursos necessários do servidor, não em níveis superiores, pois em caso de falhas na aplicação, ela somente terá acesso aos seus recursos e não aos pertencentes a outros processos.
- Não use o método GET para mandar informações sensíveis: O método GET é um mecanismo para passagens de parâmetro entre páginas WEB, as informações transmitidas podem ser facilmente capturadas, sendo que muitas vezes nem o protocolo SSL pode solucionar esse problema.
- Nunca confie nas informações fornecidas pelo usuário: As aplicações sempre devem validar as informações enviadas pelo usuário, verificando o formato e tamanho dos dados para evitar possíveis Buffers Overflows ou outros problemas.
- Não guarde as senhas de acesso ao banco de dados ou outros recursos dentro de páginas pré-processadas ou scripts cgi: Muitas vezes é possível obter o seu código fonte, obtendo-se assim senhas e outras informações sensíveis.
- Use criptografia para armazenar informações sensíveis no servidor: Dessa maneira é possível proteger números de cartão de crédito em sites de comércio eletrônico, ou qualquer outra informação importante.
- Procure não utilizar programas externos à linguagem: Em alguns casos é mais fácil utilizar chamadas a programas executáveis diretamente no sistema operacional em vez de implementar um procedimento num programa. Esse tipo de ação acaba por expor o aplicativo à falhas de segurança de outros aplicativos, como também a problemas de validação que possam permitir a execução remota de comandos.
- Não deixe comentário no código de produção: Caso possam ser visualizados eles podem auxiliar muito o trabalho de algum invasor.
- Verifique e personalize as mensagens de erro: Muitas vezes as mensagens de erro padrão de uma linguagem podem fornecer informações valiosas sobre o servidor.
- Utilize ferramentas, linguagens e bibliotecas atualizadas: Caso elas possuam algum problema de segurança todo o sistema estará comprometido.

2.4.4. Firewalls

HAZARI (2000:web) define o firewall como sendo uma barreira inteligente entre duas redes, geralmente a rede local e a Internet, através da qual só passa tráfego autorizado. Este tráfego é examinado pelo firewall em tempo real e a seleção é feita de acordo com um conjunto de regras de acesso Ele é tipicamente um roteador (equipamento que liga as redes com a Internet), um computador rodando filtragens de pacotes, um software proxy, um firewall-in-a-box (um hardware proprietário específico para função de firewall), ou um conjunto desses sistemas.

Pode-se dizer que firewall é um conceito ao invés de um produto. Ele é a soma de todas as regras aplicadas a rede. Geralmente, essas regras são elaboradas considerando as políticas de acesso da organização.

De acordo com ANONYMOUS (1999:490), podemos descrever o modelo mais comumente utilizado para implementação de um firewall:
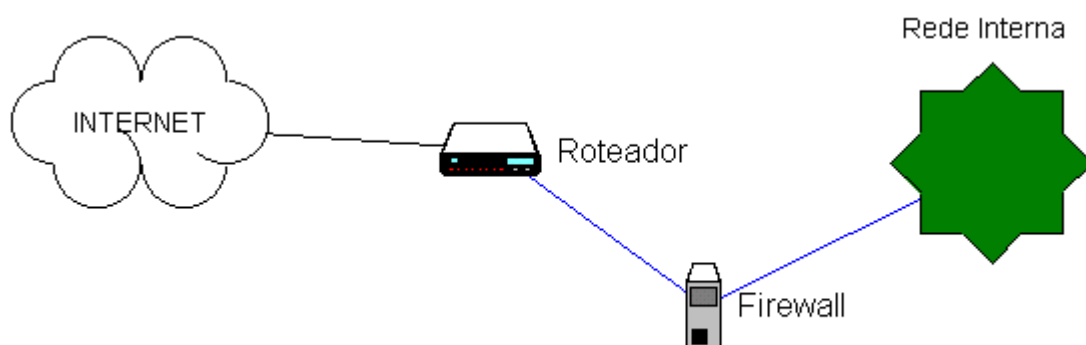
Figura 7 – Modelo Firewall

Podemos observar que o firewall é único ponto de entrada da rede, segundo ANONYMOUS (1999:488) quando isso acontece o firewall também pode ser designado como *chock point*.

De acordo com os mecanismos de funcionamentos dos firewalls podemos destacar três tipos principais:

- Filtros de pacotes
- Stateful Firewalls
- Firewalls em Nível de Aplicação

2.4.4.1. Filtros de Pacotes

Esse é o tipo de firewall mais conhecido e utilizado. Ele controla a origem e o destino dos pacotes de mensagens da Internet. Quando uma informação é recebida, o firewall verifica as informações sobre o endereço IP de origem e destino do pacote e compara com uma lista de regras de acesso para determinar se pacote está autorizado ou não a ser repassado através dele.

Atualmente, a filtragem de pacotes é implementada na maioria dos roteadores e é transparente aos usuários, porém pode ser facilmente contornada com IP Spoofers. Por isto, o uso de roteadores como única defesa para uma rede corporativa não é aconselhável.

Mesmo que filtragem de pacotes possa ser feita diretamente no roteador, para uma maior performance e controle, é necessária a utilização de um sistema específico de firewall. Quando um grande número de regras é aplicado diretamente no roteador, ele acaba perdendo performance. Além disso, Firewall mais avançados podem defender a rede contra spoofing e ataques do tipo DoS/DDoS.

2.4.4.2. Stateful Firewalls

Um outro tipo de firewall é conhecido como Stateful Firewall. Ele utiliza uma técnica chamada Stateful Packet Inspection, que é um tipo avançado de filtragem de pacotes. Esse tipo de firewall examina todo o conteúdo de um pacote, não apenas seu cabeçalho, que contém apenas os endereços de origem e destino da informação. Ele é chamado de 'stateful' porque examina os conteúdos dos pacotes para determinar qual é o estado da conexão, Ex: Ele garante que o computador destino de uma informação tenha realmente solicitado anteriormente a informação através da conexão atual.

Além de serem mais rigorosos na inspeção dos pacotes, os stateful firewalls podem ainda manter as portas fechadas até que uma conexão para a porta específica seja requisitada. Isso permite uma maior proteção contra a ameaça de port scanning.

2.4.4.3. Firewalls em Nível de Aplicação

Nesse tipo de firewall o controle é executado por aplicações específicas, denominadas proxies, para cada tipo de serviço a ser controlado. Essas aplicações interceptam todo o tráfego recebido e o envia para as aplicações correspondentes; assim, cada aplicação pode controlar o uso de um serviço.

Apesar desse tipo de firewall ter uma perda maior de performance, já que ele analisa toda a comunicação utilizando proxies, ele permite uma maior auditoria sobre o controle no tráfego, já que as aplicações específicas podem detalhar melhor os eventos associados a um dado serviço.

A maior dificuldade na sua implementação é a necessidade de instalação e configuração de um proxy para cada aplicação, sendo que algumas aplicações não trabalham corretamente com esses mecanismos.

2.4.4.4. Considerações sobre o uso de Firewalls

Embora os firewalls garantam uma maior proteção, e são inestimáveis para segurança da informação, existem alguns ataques que os firewalls não podem proteger, como a interceptação de tráfego não criptografado, ex: Interceptação de e-mail. Além disso, embora os firewalls possam prover um único ponto de segurança e auditoria, eles também podem se tornar um único ponto de falha – o que quer dizer que os firewalls são a última linha de defesa. Significa que se um atacante conseguir quebrar a segurança de um firewall, ele vai ter acesso ao sistema, e pode ter a oportunidade de roubar ou destruir informações. Além disso, os firewalls protegem a rede contra os ataques externos, mas não contra os ataques internos. No caso de funcionários mal intencionados, os firewalls não garantem muita proteção. Finalmente, como mencionado os firewalls de filtros de pacotes são falhos em alguns pontos. - As técnicas de Spoofing podem ser um meio efetivo de anular a sua proteção.

Para uma proteção eficiente contra as ameaças de segurança existentes, os firewalls devem ser usados em conjunto com diversas outras medidas de segurança.

2.4.5. Sistemas de Detecção de Intrusão - IDS

“A detecção de Intrusão é uma das áreas de maior expansão, pesquisa e investimento na segurança em redes de computadores. Com o grande crescimento da interconexão de computadores em todo o mundo, materializado pela Internet, é verificado um conseqüente aumento nos tipos e no número de ataques a esses sistemas, gerando uma complexidade muito elevada para a capacidade dos tradicionais mecanismos de prevenção. Para maioria das aplicações atuais, desde redes corporativas simples até sistemas de e-commerce ou aplicações bancárias, é praticamente inviável a simples utilização de mecanismos que diminuam a probabilidade de eventuais ataques. Um ataque

força, em casos extremos, causa interrupções totais dos serviços para que um lento e oneroso processo de auditoria e de posterior restauração manual seja feito. Isso justifica todo o investimento feito visando a criação de mecanismos que ultrapassem a barreira da simples prevenção, garantindo aos sistemas um funcionamento contínuo e correto mesmo na presença de falhas de segurança, principal objetivo dos chamados Sistemas de Detecção de Intrusão (IDS – Intrusion Detection Systems).” (CAMPELO et al, 2001:25)

Basicamente, podemos definir IDS como uma ferramenta inteligente capaz de detectar tentativas de invasão e tempo real. Esses sistemas podem atuar de forma a somente alertar as tentativas de invasão, como também em forma reativa, aplicando ações necessárias contra o ataque.

Segundo ANONYMOUS (1999:538), em função das técnicas com que os IDSs reconhecem um ataque, eles podem ser divididos em dois tipos:

- Sistemas Baseados em Regras (Rule-based systems): Esse tipo é baseado em bibliotecas ou bases de dados que contenham assinaturas dos ataques. Quando algum tráfego coincide com um critério ou regra, ele é marcado como sendo uma tentativa de intrusão. A maior desvantagem dessa técnica é a necessidade de se manter a base de dados constantemente atualizada, e além de que essa técnica somente identifica os ataques conhecidos. Além disso, às vezes pode existir uma relação inversa entre a especificação da regra e sua taxa de acerto. Isto é, se uma regra for muito específica, ataques que sejam similares, mas não idênticos, não serão reconhecidos.
- Sistemas Adaptáveis (Adaptive Systems): Esse tipo emprega técnicas mais avançadas, incluindo inteligência artificial, para reconhecer novos ataques e não somente ataques conhecidos através de assinaturas. As principais desvantagens dos sistemas adaptáveis são o seu custo muito elevado e a dificuldade no seu gerenciamento, que requer um grande conhecimento matemático e estatístico.

Além da divisão pelas técnicas de reconhecimento de ataque, os IDSs podem ser também classificados em dois tipos principais:

- NIDS - Sistemas de Detecção de Instrução de Rede
- HIDS - Sistemas de Detecção de Instrução de Host

2.4.5.1. NIDS - Sistemas de Detecção de Intrusão de Rede

A grande parte dos sistemas comerciais de detecção de intrusão é baseada em rede. Nesse tipo de IDS os ataques são capturados e analisados através de pacotes de rede.

Ouvindo um segmento de rede, o NIDS pode monitorar o tráfego afetando múltiplas estações que estão conectadas ao segmento de rede, assim protegendo essas estações. Os NIDSs também podem consistir em um conjunto de sensores ou estações espalhados por vários pontos da rede. Essas unidades monitoram o tráfego da rede, realizando análises locais do tráfego e reportando os ataques a um console central. As estações que rodam esses sensores devem estar limitadas a executar somente o sistema de IDS, para se manterem mais seguras contra ataques. Muitos desses sensores rodam num modo chamado "stealth", de maneira que torne mais difícil para o atacante determinar as suas presenças e localizações.

Segundo BECE (2001:web), podemos destacar as vantagens do IDS baseados em rede:

- A implementação de um NIDS tem pouco impacto sobre a performance da rede. Eles geralmente ficam em modo passivo, apenas escutando o tráfego da rede sem interferir no seu funcionamento.
- NIDs bem posicionados podem monitorar uma grande rede.
- Os IDSs baseados em rede podem ser muito seguros contra a maioria dos ataques, além de ficarem invisíveis aos atacantes.

E também as desvantagens:

- Os NIDs podem ter dificuldade em processar todos os pacotes em uma rede que possua um grande tráfego de dados.
- Eles não podem analisar o tráfego de informações criptografadas Esse problema vem aumentando em função da utilização de VPNs pelas organizações (e pelos atacantes também).
- Muitas vantagens dos NIDSs não se aplicam mais as modernas redes baseadas em switches. Os switches dividem as redes em pequenos segmentos (usualmente uma estação por porta) e provêm ligações lógicas diretas entre as estações no mesmo equipamento. A maioria dos switchs não tem um sistema de monitoramento de portas e isso limita ao NIDS apenas analisar uma estação. Mesmo que o switch possua o recurso de monitoramento, apenas uma porta não poderá receber todo o tráfego passando pelo equipamento.
- A maioria dos NIDSs não podem reconhecer se um ataque foi bem sucedido. Eles apenas apontam que um ataque foi iniciado. Dessa maneira eles apenas detectam um ataque, sendo que o administrador de sistemas deve verificar se o host apontado foi atacado.
- Alguns IDSs baseados em rede têm problemas em lidar com pacotes de dados fragmentados. Esses tipos de pacotes podem até tornar um NIDs instável ou mesmo travar o seu funcionamento.

2.4.5.2. HIDS - Sistemas de Detecção de Instrução de Host

Os HIDSs operam sobre informações coletadas em computadores individuais. Através disso os HIDs podem analisar as atividades das estações com confiança e precisão, determinando exatamente quais processos e usuários estão envolvidos em um tipo particular de ataque no sistema operacional. Além disso, ao contrário dos sistemas baseados em rede, os baseados em host (estação) podem ver as conseqüências de uma tentativa de ataque, como eles podem acessar diretamente e monitorar os arquivos e processos do sistema usualmente alvos de ataques.

Alguns HIDSs suportam um gerenciamento centralizado e relatórios que podem permitir que um apenas um console possa gerenciar várias estações. Outros geram mensagens em formatos que são compatíveis com os sistemas de gerenciamento de redes.

Segundo BECE (2001:web), podemos descrever as vantagens dos IDSs baseados em host:

- Esse tipo de IDS tem a capacidade de monitorar eventos locais de um host, podendo detectar ataques que não poderiam ser detectados por um IDS de rede.
- Eles podem operar em um ambiente onde o tráfego de rede é criptografado, a informação é analisada antes de ser criptografada na origem, ou depois de ser decriptada no destino.
- Quando o IDS de host opera em nível de sistema operacional, ele pode ajudar a detectar 'Trojan Horses' ou outros tipos de ataques que envolvam problemas de integridade nos programas.

E também as desvantagens:

- Esse tipo de IDS é difícil de se gerenciar porque cada host monitorado precisa ser configurado.
- Como as informações utilizadas para análise do HIDS estão armazenadas no host, um atacante pode invadir o sistema e desabilitar essas funcionalidades.
- Os HIDSs não podem reconhecer ataques que sejam destinados a rede inteira porque apenas conseguem monitorar os pacotes de redes recebidos pelo próprio host.
- Um IDS baseado em host consome recursos de processamento do host monitorado, influenciando na sua performance.

2.4.6. Logs e Auditoria

"Imagine que você chegue em sua casa e perceba que ela foi aparentemente violada. O que você faz? Procura por pistas como: vidros quebrados, marcas na maçaneta, trincos forçados, portas arrombadas, objetos desaparecidos, em resumo, sinais que caracterizem e permitam estabelecer a magnitude da violação. Analogamente, nos sistemas computacionais, intrusos deixam pistas, porém, diferente do "mundo real", as pistas estão nos registros de atividades do sistema, o qual denominamos de *logs*. Melhor ainda, os *logs* podem desempenhar um papel preventivo, na medida em que podem registrar as eventuais tentativas de ataque. " (ALEGRE, 1999:web)

De uma maneira simples, os logs são quaisquer registros, gerados pelo sistema operacional ou aplicações, com informações sobre os eventos ocorridos para uma posterior verificação. Apesar de ser uma medida de segurança básica, muitos esquecem dos arquivos de logs; eles são uma das formas mais elementares de auditoria de sistemas.

Normalmente os logs são gerados pela maioria dos equipamentos de rede. Além disso, todos os sistemas operacionais têm no mínimo ferramentas gerais para geração dos logs, que são habilitadas durante uma instalação normal do sistema.

Os logs são extremamente importantes por três razões principais. Primeira, eles podem fornecer uma visão das atividades que estão ocorrendo nos sistemas. Segunda, eles podem fornecer dados para análises de detecção de problemas ou falhas de segurança nos sistemas. Teceira, talvez a mais importante, os logs podem ser utilizados como evidências de um incidente de segurança.

Os logs podem fornecer informações valiosas, mas que muitas vezes são ignoradas pela falta de tempo para revisar tantas informações. O mais indicado é automatizar o processo de forma que torne mais fácil a verificação dos logs, somente as informações necessárias são extraídas e notificadas. Além desse processo de filtragem podem ser consideraras outras recomendações sobre a utilização dos logs, de acordo com ALEGRE (1999:web):

- Crie uma política de *logs* séria, identificando: os tipos de informação que podem ser registrados, os mecanismos para tal registro, onde essa tarefa será realizada e onde os arquivos de *logs* serão armazenados.
- Determine se os mecanismos providos pelo seu sistema, e na rede de maneira geral, registram as informações necessárias.
- Habilite os mecanismos de *logs*. Recomenda-se em uma primeira instância registrar o máximo de *logs* possíveis, e posteriormente, determinar que dados são mais significativos dentro de um processo de detecção de intrusão.
- Monitore os arquivos de *logs* regularmente em busca de atividades suspeitas.

- Investigue qualquer anomalia encontrada, isto é, verifique se ela pode ser atribuída a algum tipo de atividade autorizada, por exemplo: o usuário realmente estava em Toronto no dia anterior e conectou-se no sistema? Ou houve realmente uma queda de energia que fez com que o sistema seja reinicializado?
- Caso seja confirmada qualquer evidência (ou tentativa) de intrusão, contacte seu respectivo grupo de segurança e reporte o incidente ou, se este grupo não existir, contate diretamente os responsáveis técnicos das redes comprometidas. Inclua na mensagem os *logs* e o seu *timezone*.
- Recomenda-se criar ou fazer uso de *scripts* que facilitem a tarefa de análise diária de *logs* ou lançar mão de um analisador de *logs* (*log analyzer*).
- Ao examinar sinais de intrusão, lembre-se que a informação de uma fonte pode não parecer suspeita por si mesma. Inconsistências entre diversas fontes podem ser, às vezes, a melhor indicação de atividade suspeita ou intrusões.
- Faça backup dos seus *logs* periodicamente.
- Sincronize todas as suas máquinas e dispositivos de rede com servidores de tempo (servidores NTP) de forma a unificar o *timestamps* dos *logs*.
- Recomenda-se, fortemente, a implementação de um sistema de *logs* centralizado (*loghost*).
- Acompanhe regularmente alertas e boletins de segurança emitidos por fontes confiáveis. Isto aumentará seu conhecimento sobre os mecanismos de ataque mais recentes e fará com que você se aperfeiçoe na procura de atividade suspeita.
- O uso de ferramentas que automatizem/auxiliem no trabalho de coleta, análise e monitoramento de *logs* é altamente recomendado.

Os *logs* desempenham um papel imprescindível no processo de detecção de intrusão. A auditoria e avaliação destes devem se tornar rotineiras e uma constante na vida dos administradores a fim de evitar surpresas desagradáveis.

2.4.7. Recuperação de Desastres e Backup

Podemos definir recuperação de desastres como o processo de restauração do sistema após a perda de dados.

ANONYMOUS (1999:553), descreve as principais ameaças que podem causar um desastre a um sistema:

- Força Maior: Ações da Natureza (Erupções vulcânicas, incêndios, enchentes, terremotos, furacões ou maremotos) podem acabar totalmente os equipamentos e conseqüentemente com os dados.
- Erros inocentes: Usuários autorizados podem inadvertidamente destruir ou sobrescrever dados vitais enquanto estiverem administrando os sistemas.
- Falhas Mecânicas: Na era do hardware barato, produção em massa de hardware, falhas mecânicas são comuns. Um harddisk novo às vezes pode simplesmente falhar, por exemplo.
- Falhas em programas: algum programa que possua falhas ou erros de programação pode danificar dados importantes.

Essas ameaças, além de vírus, ataques ou qualquer outra atividade maliciosa influenciam diretamente, em vários níveis, na operação de uma empresa, desde uma estação individual até uma rede corporativa inteira. Quando algum desastre acontece, ao invés de se descobrir à origem, o foco principal é restaurar os recursos de tecnologia da informação para sua total funcionalidade, restaurando as operações do negócio. Quanto maior for a demora, maiores serão as conseqüências para a empresa.

Backups diários ou semanais dos sistemas, incluindo dados essenciais para operação da empresa, são componentes vitais para restauração de desastres e para manutenção das funções da empresa.

Apesar de ser uma medida de segurança antiga, muitas empresas não possuem um sistema de backup ou, o fazem de maneira incorreta.

Montar um sistema de backup requer um pouco de cautela. É importante, por exemplo, saber escolher o tipo de mídia para se armazenar as informações, como fitas magnéticas, discos óticos ou sistemas RAID. O dispositivo mais usado é o DAT (Digital Audio Tape), pois oferece capacidade de armazenamento de até 8GB, a um custo médio muito baixo.

Embora as mídias óticas se mostrem como última palavra em backup, não são muito viáveis, pois possuem capacidade de armazenamento relativamente pequena (cerca de 600 MB em um CD). Um ponto a favor das mídias óticas é a segurança, porém atualmente estão sendo utilizadas para a criação de uma biblioteca de dados, o que caracteriza armazenamento de dados e não, backup.

A tecnologia RAID, segundo o site AC&NC na sua seção Raid.edu (2001:web), consiste num conjunto de drives que é visto pelo sistema como uma única unidade, continuando a propiciar acesso contínuo aos dados mesmo que um dos drives venha a falhar. Os dados passam pelo nível 1, que significa espelhamento de drives ou servidores (cópia dos dados de drives ou servidores), até o nível 5, que é o particionamento com

paridade (o mesmo arquivo repetido em diferentes discos). Esta tecnologia é uma opção segura e confiável, sendo muito utilizada em empresas que possuem rede non-stop e que não podem perder tempo interrompendo o sistema para fazer backup, entretanto ela garante apenas a segurança contra problemas físicos no equipamento.

Outro ponto muito importante e que é sempre bom lembrar, é que a maioria de falhas nas redes corporativas é fruto de erro humano. Isto significa que é necessário um treinamento dos envolvidos, para que estes possam agir de maneira correta em caso de emergência (restauração do backup).

Entre as falhas mais comuns, além da falta de preparo dos envolvidos, é o armazenamento dos disquetes ou outra mídia de armazenamento no próprio local onde se localiza o computador, o que no caso de qualquer desastre (incêndio, enchente, etc...), levará a perda total dos dados. O mais indicado é a utilização de dois conjuntos de backups: um disponível localmente para o uso imediato, e um conjunto guardado em um local diferente da empresa com informações referentes à no mínimo uma semana.

Além disso, JOHNSON (2000:web) descreve alguns fatores devem ser considerados sobre a segurança no processo de backup e restauração:

- Realize backups usando dispositivos locais ao invés de transmitir os dados pela rede.
- Se possível, encripte os dados armazenados nos backups.
- Limite o número de pessoas que tem acesso ao backup ou a funções de restauração dos dados.
- Nunca realize backups de arquivos ou banco de dados de segurança (arquivos de senhas, chaves de criptografia, etc…) através da rede.
- Sempre mantenha registros bem documentados sobre os dados armazenados nos backups.

O processo de backup é muito importante para a recuperação de desastres e para o funcionamento de uma empresa. Deve-se ter um plano de ação para montar um sistema de backup, ou seja, as estratégias tanto de emergência quanto a da própria rotina devem ser estudadas e padronizadas para que todos estejam preparados.

2.4.8. Proteção Contra Malware

Na maioria das vezes, para se infectar uma máquina é preciso uma pessoa com motivação para abrir um arquivo. Por isso, uma das causas principais de infecção apontadas

por especialistas é a falta de conhecimento aliada à curiosidade dos usuários. De acordo com o site da empresa de segurança MÓDULO (2001:web), podem ser destacados alguns procedimentos para se manter protegido contra os vírus:

- Se você trabalha com Windows, sempre cheque os patches de segurança. Algumas versões do sistema, como o Windows ME, fazem atualizações automáticas. A dica vale também para outros sistemas operacionais.
- Não abra arquivos anexados que você não esteja esperando, especialmente se ele vier de alguém que você não conheça.
- Use e abuse de antivírus. Há versões gratuitas na rede, mas com uso limitado de tempo. A compra de um antivírus pode garantir mais tranqüilidade.
- Comprar um software de proteção não é suficiente. É preciso atualizá-lo, já que novas pragas são descobertas praticamente todos os dias.
- Especialistas têm indicado a instalação firewall pessoal, especialmente para os usuários de conexões rápidas como via cabo.

2.4.9. Política da Segurança

"A política de segurança da informação é o conjunto de diretrizes que deve expressar o pensamento da alta administração da organização em relação ao uso da informação por todos aqueles que têm acesso à esse bem. Neste caso, a administração está representando os acionistas que, como donos, devem decidir os destinos de todos os recursos da organização." (FONTES, 2000:web)

Dessa maneira podemos definir a política da segurança como sendo sistemáticas gerenciais que visam determinar o nível de segurança de uma rede ou sistemas de informação de uma organização, suas funcionalidades e a facilidade de uso.

Essas sistemáticas são reunidas em um documento formal com regras pelas quais as pessoas deverão aderir para ter acesso à informação e à tecnologia de uma empresa.

Para se estabelecer uma política de segurança é necessário conhecer os objetivos da organização, para depois poder medi-los e verificar as ameaças.

Segundo FONTES (2000:web) a política de segurança deve ser desenvolvida segundo algumas características, tais como :

- Ser complementada com a disponibilização de recursos: Uma ação concreta de que a política é levada a sério pela direção é a liberação de recursos financeiros e de pessoal para que as diretrizes descritas possam ser implementadas ao longo do tempo. O ritmo dessa implementação dependerá de cada organização.

- Ser verdadeira A política deve realmente exprimir o pensamento da empresa e deve ser coerente com as ações dessa organização. Deve ser possível o seu cumprimento.
- Ser curta: Duas a três páginas são suficientes para se formalizar uma política. Não devemos confundir política com normas e procedimentos de segurança. A política não deve ser um Manual de Procedimentos. Este manual pode até existir, mas terá vida própria.
- Ser válida para todos: A política deve ser cumprida por todos os usuários que utilizam a informação da organização. Ela é válida para o presidente e para o estagiário recém contratado. Normalmente o "rei" não causa maiores problemas. Os problemas deste tipo são causados pelos "amigos do rei".
- Ser simples: A política deve ser entendida por todos. Deve ser escrita em linguagem simples e direta. A política não deve conter termos técnicos de difícil entendimento pelos "mortais".
- Ter o patrocínio da alta direção da organização O documento normativo que formalizará a política deve ser assinado pelo mais alto executivo, explicitando assim o seu total apoio à política.

As políticas variam de organização para organização, porém alguns pontos comuns a todas as organizações devem ser tratados:

- A Informação como um Bem da Empresa - uso profissional;
- Controle do acesso à Informação;
- Gestor da Informação;
- Responsabilidades - usuário, gerência e Gestor da Informação;
- Preparação para situações de contingência - continuidade operacional;
- Privacidade do usuário - arquivos pessoais, correio eletrônico;
- Medidas disciplinares que serão utilizadas caso a Política não seja cumprida.

A política de segurança proporciona o direcionamento para as implementações técnicas. Implementar procedimentos de segurança sem uma política definida é equivalente a navegar sem saber onde se quer chegar. Porém a política deve ser um elemento de um conjunto de ações que compõem o Processo de Segurança da Organização.

Sempre devemos ter em mente que para se ter a proteção efetiva da informação da organização, é necessário a existência de um conjunto de ações que permitirá o alcance deste objetivo. Nenhum elemento isolado conseguirá esta façanha. A segurança é como uma corrente, formada por vários elos e a força dessa corrente será medida pela resistência do seu elo mais frágil.

2.4.10. Plano de Resposta a Incidentes

Mesmo a melhor infraestrutura de segurança da informação não pode garantir que intrusos ou outras ações maliciosas ocorram. Quando um incidente de segurança ocorre, é um fator crítico para organização ter meios para responder a esse evento. A velocidade a qual uma organização pode reconhecer, analisar, e responder a um incidente de segurança limita os estragos e diminui os custos de restauração. A habilidade de usar essa informação para preparar ou prevenir ocorrências similares aprimora a segurança geral de uma organização.

O Plano de Resposta a Incidentes é um documento que descreve as diretrizes gerais e procedimentos para tratamento dos principais incidentes de segurança que podem ocorrer na organização, promovendo ao pessoal de suporte instruções sobre as medidas a serem tomadas para a identificação e correção dos mesmos.

O tipo de tratamento dado aos incidentes de segurança varia de acordo com a sua intensidade e risco. Porém, o encaminhamento deve ser decidido em acordo com a alta direção da empresa e com o respaldo do departamento jurídico. As ações pertinentes podem envolver o relacionamento com entidades externas (como clientes, parceiros, provedores de serviços, etc.) ou mesmo exigir o acionamento de autoridades e órgãos policiais.

Principais pontos a serem considerados em um Plano de Resposta à Incidentes:

- Procedimentos para identificação e auditoria dos problemas
- Divulgações das Informações
- Procedimentos e Pessoal responsável pela restauração dos sistemas
- Contatos com as fontes do ataque e com os órgãos de segurança
- Procedimentos para isolamento dos sistemas

CAPÍTULO 3 – DESCRIÇÃO PRÁTICA

Uma vez abordada a fundamentação teórica necessária, cabe agora descrever as atividades desenvolvidas no campo de estágio e sua relação com toda teoria obtida através da Universidade, de cursos extracurriculares, de estudos e pesquisas.

A etapa do estágio é, sem dúvida, a mais importante, já que é através das atividades práticas vivenciadas em campo que estes conceitos se consolidarão em uma experiência profissional duradoura.

3.1. O Processo de Estudo

Apesar da existência de uma grande experiência profissional nas tecnologias aplicadas no desenvolvimento do estágio, uma parte do tempo foi destinada ao estudo das tecnologias envolvidas. Portanto, cabe apresentar este processo de estudo que iniciou a partir da definição do tema a ser apresentado no estágio, em função da necessidade da empresa em garantir maior segurança para seus servidores.

3.1.1. Adquirindo Conhecimentos sobre a Segurança para o Comércio Eletrônico

Quando o objetivo é proteger algum recurso em tecnologia da Informação, o primeiro passo necessário é conhecer profundamente o seu funcionamento. Como o objetivo inicial da empresa seria tornar mais seguras as transações de comércio eletrônico realizadas através de seu sistema, nessa fase foram estudadas as principais formas de comércio eletrônico e suas características de segurança. Foram observados diversos sites, e os recursos utilizados para garantir a segurança. O estudo foi ambientado basicamente no segmento Business to Consumer (B2C – Empresa – Consumidor), ao qual o sistema da empresa foi desenvolvido. Foram estudados recursos de segurança para envio das informações pela Internet (Protocolo SSL), para os sistemas de pagamento (Protocolo SET, Cartão de Crédito, Boleto ou Depósito Bancário) e as formas de proteção dos dados armazenados (Criptografia Assimétrica).

3.1.2. Aprofundando Conhecimento em Segurança no Linux

Como toda a plataforma de servidores da Empresa é baseada no sistema operacional Linux, e conseqüentemente o sistema desenvolvido roda sobre essa plataforma, tornou-se necessário aprofundar os conhecimentos sobre a segurança desse sistema operacional e as ferramentas de segurança disponíveis.

Sendo assim, podem ser destacados os principais pontos estudados sobre a segurança do sistema operacional Linux:

- Sistema de controle de usuários e senhas;
- Sistema de permissões de arquivos;
- Recursos de segurança em rede;
- Sistema de registro de Logs;

Mesmo com a experiência anterior como Administrador de Sistemas na Empresa, essa fase foi de grande valia porque permitiu o conhecimento de diversas novas ferramentas de segurança disponíveis para proteção do sistema.

3.1.3. Aprofundando Conhecimentos em Criptografia

O estudo inicial sobre segurança para o Comércio Eletrônico havia contribuído com novos conceitos e tecnologias sobre o uso e aplicação da criptografia, como o processo de certificação digital e o sistema de pagamento SET. Sendo assim, nesta fase essas tecnologias foram intensivamente estudadas e conceitos já conhecidos anteriormente foram reforçados. Na aplicação prática, a criptografia foi utilizada para proteção da comunicação entre os servidores, para a segurança das transações de comércio eletrônico, armazenamento dos backups e gerenciamento dos servidores, como poderá ser constatado no tópico 3.4.7 – Criptografia para Proteção dos Dados.

3.1.4. Estudos das Ameaças e Técnicas de Ataque

Essa foi uma das fases mais intrigantes do desenvolvimento prático do estágio. Nela foram estudas as ameaças à segurança da tecnologia da informação e as principais técnicas de ataque utilizadas por hackers. Através do conhecimento obtido nessa fase, puderam ser identificadas vulnerabilidades antes desconhecidas nos sistemas da empresa, as quais serão definidas no tópico 3.2.1 – Análise de Vulnerabilidades.

3.1.5. Aprofundando Conhecimentos sobre as Medidas e Ferramentas de Segurança

Nessa fase foram reforçados os conhecimentos sobre as medidas e ferramentas de proteção da segurança. Foram testadas e analisadas as ferramentas necessárias para a eliminação das ameaças estudadas anteriormente, além do estudo de técnicas para identificação das vulnerabilidades. Para realização dos testes foi utilizada uma máquina específica para essa função, onde foram estudados o funcionamento e as configurações dessas ferramentas, para então serem aplicadas aos equipamentos em operação. As ferramentas escolhidas e os requisitos considerados para seleção serão descritos no tópico 3.3.3 – Escolha das Ferramentas.

3.2. Levantamento da Estrutura Atual

Antes de iniciar qualquer ação que busque a segurança em um ambiente computacional, é necessário conhecer as características atuais desse ambiente. Conhecer aspectos relacionados à estrutura lógica e de rede pode ajudar na descoberta de vulnerabilidades desse ambiente, além de auxiliar na determinação das estratégias a serem adotadas.

Dessa maneira, através do modelo abaixo podemos demonstrar como estão organizados: a rede, os computadores e servidores da empresa:
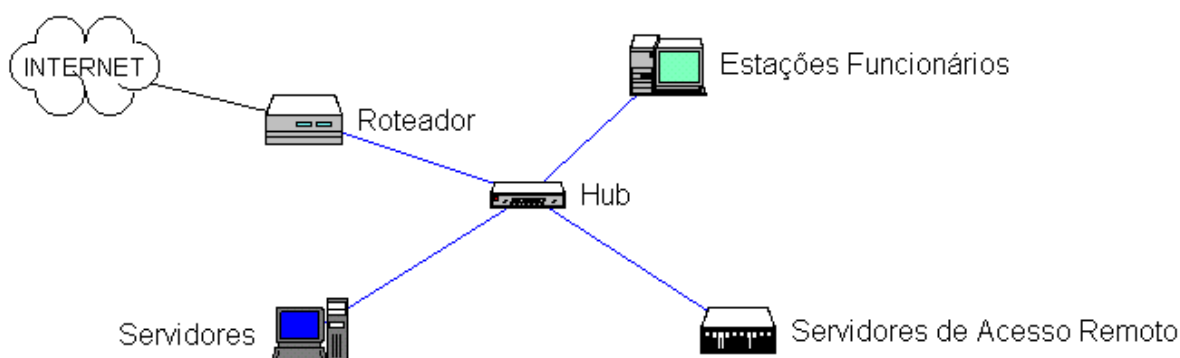
Figura 8 – Estrutura da Rede

Através da figura podemos observar que toda a rede está interligada através de um HUB[4] Ethernet[5]:

Qualquer informação vinda da Internet passa pelo roteador e em seguida já está disponível na rede, o único controle do tráfego é feito através de algumas regras acesso configuradas diretamente no roteador.

Os servidores de acesso remoto (RAS – Remote Access Servers) são responsáveis por fornecer o serviço de acesso discado aos usuários do provedor, eles possuem modems digitais integrados e estão ligados diretamente na rede. Após o usuário estar conectado ao provedor, as suas informações são enviadas através do RAS para o HUB, e então são repassadas para o roteador.

As estações funcionam com o sistema operacional Microsoft Windows 98 SE (Segunda Edição). Elas são utilizadas pelos funcionários para o compartilhamento de arquivos e impressoras, além de darem suporte aos sistemas administrativos da empresa. As estações ainda possuem software antivírus que é constantemente atualizado através da Internet, dessa maneira podem ser identificados os vírus e worms mais atuais.

---

[4] HUB equipamento de rede responsável por repetir os dados recebidos para os outros hosts.

[5] ETHERNET é um padrão de redes criado pela Xerox. É o padrão mais comum encontrado em redes locais.

Todos os servidores rodam o sistema operacional Linux, freqüentemente atualizado, e são responsáveis por fornecer informações tanto para os usuários, funcionários e acessos vindos pela Internet. Os seus serviços estão distribuídos da seguinte maneira:

Relação de Servidores

CPU (MHz)	RAM (MB)	Serviços
Pentim III 500	512	Servidor WEB, E-mail, Banco de Dados
Pentim II 300	128	Autenticação, Cache
AMD K6-2 300	64	Servidor de Banco de Dados Interno
AMD K6-2 300	128	Servidor de FTP

Tabela 2 – Relação de Servidores

Os registros de acesso e funcionamento (logs) dos servidores ficam armazenados localmente nos próprios equipamentos, e são gravados no backup em CD-RW realizado diariamente.

3.2.1. Análise de Vulnerabilidades

A Análise de vulnerabilidades permite detalhar as falhas de segurança encontradas numa organização, para que posteriormente ações de correção possam ser tomadas.

Numa situação ideal, a análise deveria iniciar antes da rede se tornar operacional, apenas com computadores e equipamentos individuais, falhas de segurança deveriam ser corrigidas antes deles serem conectados à rede. Mas na realidade, já existem computadores e equipamentos conectados em rede e a uma conexão Internet, as suas vulnerabilidades devem ser identificadas e eliminadas.

Nesse sentido, após termos compreendido a estrutura atual da empresa, pode-se descrever as principais vulnerabilidades encontradas:

1) Os HUBs Ethernet são equipamentos que atuam apenas no nível físico, eles repetem todos os pacotes de rede recebidos em todas as suas portas, ficando como função das placas de rede processarem apenas os pacotes destinados a elas.

   Dessa forma, se qualquer computador ou equipamento for invadido, um sniffer poderia ser instalado para monitorar todo o tráfego dessa rede. Isso é extremamente grave porque além de todo o tráfego não criptografado, poderiam ser capturadas senhas de acesso aos servidores e dados dos sistemas administrativos da empresa.

2) Apesar dos programas dos servidores serem atualizados com freqüência para solução de problemas de segurança, esse processo não ocorre com a devida agilidade. Muitas vezes o tempo entre o anúncio de um problema de segurança e a sua atualização acaba por se estender demais, devido a grande carga de trabalho dos administradores de sistemas da empresa.
3) O fato dos logs estarem armazenados localmente nos servidores poderia facilitar o trabalho de um invasor. Caso alguma máquina fosse comprometida, o invasor poderia apagar dos logs todos os indícios de seu acesso, antes mesmo da cópia desses logs serem armazenadas no backup.
4) O ponto de entrada da rede é o roteador, apesar dele possuir algumas regras de acesso configuradas, um firewall poderia oferecer uma proteção bem maior. Além disso, quanto mais regras forem adicionadas ao roteador, maior será a sua perda de performance.
5) Não é utilizado nenhum tipo de ferramenta IDS para auxiliar no processo de identificação de intrusão. Dessa forma os ataques dificilmente podem ser reconhecidos no momento de sua execução.
6) Caso ocorresse algum tipo de incidente, como a invasão de um servidor, ações incorretas poderiam acabar prejudicando ainda mais a situação. Não há nenhum documento descrevendo os procedimentos necessários e as pessoas responsáveis para tratar desse incidente, ou seja, não existe um Plano de Resposta à Incidentes.

3.3. Escolha das Ferramentas

Nesta fase, foram determinados os sistemas de segurança a serem aplicados. Foi realizada uma extensa pesquisa em vários sites sobre segurança para a definição dessas ferramentas, sendo que os principais pontos considerados na escolha foram a facilidade de uso, eficiência e capacidade de atualização. Devido a política da empresa definir a utilização preferencial de programas Open Source, ou também Freewares, em nenhum momento, além do uso do Anti-vírus, foi considerada a utilização de ferramentas comerciais. A preferência da empresa por esses tipos de programas se dá por três motivos principais:

- Ausência de custos de aquisição, já que os programas são de livre distribuição;
- Flexibilidade dos programas de código aberto (Open Source), a qual permite a implementação de novas funções considerando as necessidades da empresa;
- Possibilidade de auditoria nos fontes dos programas de código aberto, permitindo que sejam verificadas falhas de segurança ou códigos maliciosos inseridos pelos desenvolvedores desses programas;

Seguindo esses requisitos, as ferramentas selecionadas seguem na tabela abaixo:

Ferramenta	Categoria	Site
AVP	Anti-vírus	http://www.kaspersky.com
Gnupg	Criptografia Assimétrica	http://www.gnupg.org
Ipchains	Firewall Linux Kernel 2.2.x	http://netfilter.filewatcher.org/ipchains
ModSSL	Criptografia SSL	http://www.modssl.org
Nessus	IDS de Rede	http://www.nessus.org
Nmap	Port Scanning	Http://www.insecure.org/nmap
Snort	IDS de Rede	http://www.snort.org
Syslogng	Ferramenta de Logging	http://www.syslogng.org
Tripwire	IDS de Host	http://www.tripwire.org
Vtun	Virtual Private Network	http://vtun.sourceforge.net

Tabela 3 – Ferramentas Escolhidas

A utilização dessas ferramentas será descrita no decorrer do processo de implantação.

3.4. Implantação

Essa fase busca, além de eliminar as vulnerabilidades encontradas anteriormente, realizar ações com intuito de garantir um maior nível de segurança para os servidores e a rede da empresa, assim dando suporte ao comércio eletrônico e aumentando a segurança da organização.

3.4.1. Segmentação da Rede

Uma das maiores vulnerabilidades da estrutura da rede era a utilização de um HUB que centralizava e repetia todo o tráfego da rede. Dessa maneira a primeira ação realizada foi a segmentação do tráfego em três redes distintas: rede de servidores, rede com as estações dos funcionários e a rede dos RASs.

Para realizar essa divisão foi posicionado um firewall com quatro placas de rede entre os segmentos, três placas conectadas a cada novo segmento de rede e uma placa

conectada diretamente ao roteador. Podemos visualizar como ficou organizada a nova estrutura através da figura a seguir:
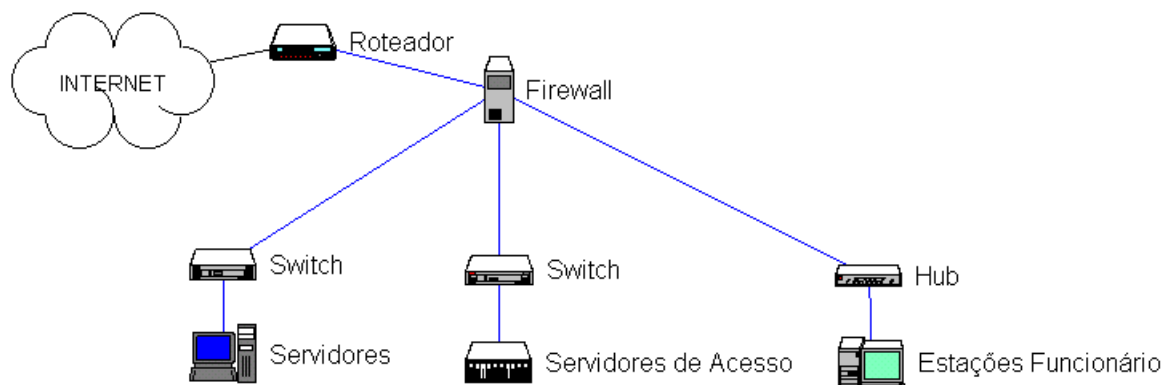
Figura 9 – Segmentação da Rede

Com a criação dos segmentos de rede distintos foi necessária a compra de novos equipamentos para permitir a conexão dos computadores e equipamentos. O antigo HUB foi utilizado no segmento das estações dos funcionários, sendo assim necessário adquirir dois novos equipamentos para fornecer as conexões de rede dentro dos segmentos de servidores e servidores de acesso. Ao invés de serem utilizados HUBs, nessas sub-redes foram utilizados Switches para garantir uma maior proteção contra o uso de Sniffers. Ao contrário dos HUBs onde todos os pacotes recebidos são encaminhados para todas as estações conectadas à rede local, os Switches direcionam cada pacote recebido de uma das suas portas para uma porta específica de saída, para encaminhamento a seu destinatário final.

3.4.2. Controle do Tráfego de Informações

Com o firewall posicionado estrategicamente entre as sub-redes e a Internet, tornou-se possível controlar todo o tráfego entre essas redes e a sua comunicação com a Internet, fornecendo um controle incomparável com a situação encontrada anteriormente. Nesse equipamento foi utilizado o sistema operacional Linux com o seu sistema de firewall de filtro de pacotes, IPCHAINS, original dos kernels da série 2.2.x. Foram criadas regras que especificavam que todo tráfego que não for expressamente permitido, é proibido. Essas regras controlam tanto todas as informações recebidas através de cada interface de rede como o tráfego de saída. No caso do tráfego originado da Internet para os servidores de acesso remoto, essas regras tiveram de ser praticamente nulas, pois os usuários do

provedor, que se conectam a esse equipamento, não podem ter nenhuma restrição de acesso aos recursos da Internet.

Além do controle oferecido pelo firewall, foram adicionadas novas regras de acesso no roteador, permitindo o controle diretamente na entrada das informações vindas da Internet. No roteador foram colocadas proteções contra IP Spoofing, onde eram negadas informações vindas da Internet com endereços de origem da própria empresa, e informações com destino à Internet com endereço de origem diferente da empresa. Dessa maneira foi possível eliminar a ameaça de IP Spoofing vindas de atacantes pela Internet, como também o uso de IP Spoofing por parte dos usuários ou funcionários da Empresa. Também foram adicionadas regras de acesso para negar informações com endereços IP reservados. Os endereços de classes reservadas são destinados para serem utilizados somente em redes locais e não podem ser roteados através da Internet, muitos dos ataques DoS e DDoS utilizam esses endereços para ocultar a sua origem. No roteador ainda foram adicionadas regras para impedir ataques DDoS originados na empresa, e regras de acesso aos servidores e servidores de acesso remoto, não estendendo muito o nível de controle, pois já havia sido comprovado que um grande número de regras no roteador poderia afetar a sua performance.

O maior nível de proteção foi aplicado ao segmento de servidores, somente o tráfego correspondente aos serviços disponíveis nesses servidores é autorizado. Além do controle oferecido pelo roteador e pelo firewall, foram utilizadas regras de acesso locais em cada servidor. Como todos eram baseados no sistema operacional Linux, que por sua vez já tem o recurso de filtragem de pacotes integrado ao kernel, cada servidor foi configurado para filtrar as informações recebidas e enviadas. Dessa maneira, mesmo que um invasor viesse a passar pelos filtros designados pelo roteador e pelo firewall, acabaria sendo barrado pelos filtros locais dos servidores. Além disso, a relação de confiança de acesso entre os servidores ficou extremamente restrita. Mesmo que um servidor fosse comprometido, através dele não se teria acesso total aos outros servidores do segmento.

De uma maneira simples, podemos observar esquema filtragem através da Figura 10, que se encontra na página seguinte.
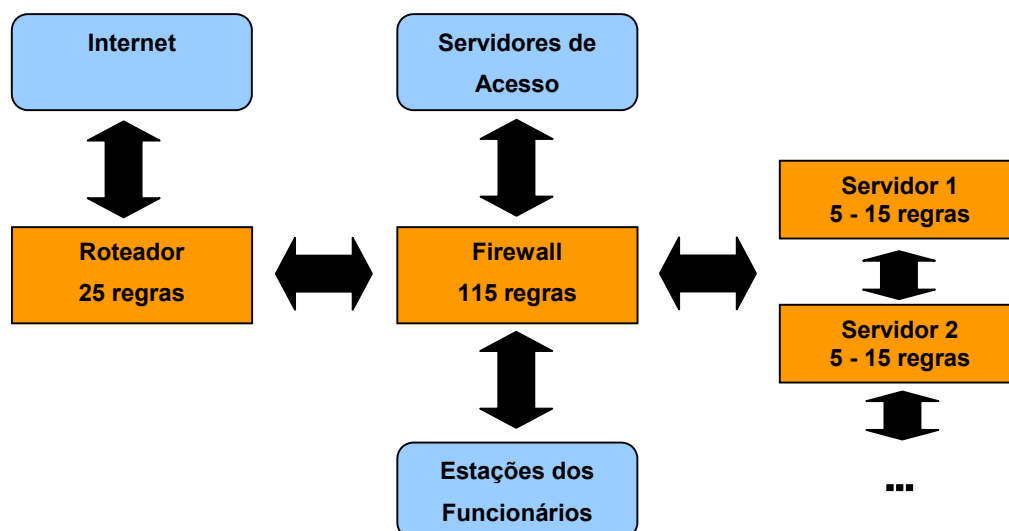
Figura 10 – Controle do Tráfego

Os itens em laranja representam os pontos onde a informação é analisada através das regras de acesso, as setas indicam que a informação pode estar trafegando em ambos os sentidos.

Como pode ser observado, foi necessária a criação de um grande número de regras de acesso para controle do tráfego. Devido à complexidade encontrada, a aplicação dessas regras em conjunto ao processo de segmentação da rede, foram os processos que mais ocuparam recursos de tempo para sua execução. Diversos ajustes tiveram de ser feitos até o ambiente tornar-se completamente operacional, sem problemas.

Finalmente, nesta fase foi utilizado o programa de Port Scaning NMAP a partir de vários pontos da rede, inclusive através da Internet. Ele permitiu verificar se as regras estavam aplicadas de forma correta, apontando quais informações poderiam passar, ou não, através do firewall.

3.4.3. Preparação dos Servidores

Para execução do novo sistema de comércio eletrônico, foi considerada a utilização de um servidor independente. Os outros servidores compartilhavam serviços que eram utilizados pelos usuários do provedor, tornando mais difícil garantir a segurança. Além disso, quanto maior o número de serviços em um servidor, maior a probabilidade de ser descoberta uma falha de segurança em seus sistemas. Sendo assim foi instalado e devidamente configurado um servidor específico para o comércio eletrônico.

Esse novo servidor fornece apenas os serviços de Servidor WEB com criptografia SSL e Servidor de Banco de Dados. Ele utiliza um sistema de RAID 1 que faz o espelhamento de discos para garantir a disponibilidade da informação no caso de uma falha física em algum dos discos rígidos.

Todos os demais servidores passaram por um processo onde foram removidos programas e contas de usuários não utilizados, e as configurações dos programas foram verificadas em busca de erros que pudessem facilitar algum acesso.

Além disso, os procedimentos de atualização de todos os servidores foram revisados a fim de garantir maior velocidade no processo. A responsabilidade por manter os servidores atualizados foi repassada para outras pessoas que também deveriam se manter informadas sobre os problemas e providenciar as correções o mais rápido possível.

3.4.4. Procedimentos de Backup

Foram criados scripts para automatizar todo o processo de backup. Eles automaticamente copiam e compactam os dados, que logo após são enviados para a estação que armazena esse backup em CD-RWs.

São realizadas cópias diárias e semanais, sendo que as cópias semanais sempre são geradas em duplicidade. Uma cópia fica disponível na própria empresa e a outra cópia é levada por um dos sócios para outro local onde ela é guardada num cofre. Dessa maneira essa cópia reserva fica protegida contra desastres naturais, roubos ou a qualquer outro incidente físico que possa ocorrer à empresa.

Para finalização dessa fase foi criado um documento chamado "Manual de Procedimentos de Backup" que descreve todas as ações e os responsáveis envolvidos no processo de backup dos sistemas.

3.4.5. Fortalecimento de Senhas

As senhas são uma forma de controle de acesso aos recursos de um sistema ou uma rede. Entretanto, se elas não forem aplicadas corretamente, podem deixar um sistema ou uma rede ainda mais vulnerável.

Sendo assim, foi necessário que alguns procedimentos referentes à escolha e utilização das senhas fossem reformulados na empresa.

A primeira ação realizada foi a troca das senhas atuais de todos os servidores e estações. Para escolha das novas senhas foi utilizado um programa que tem a função de

gerar randomicamente senhas (Random Password Generator), esse tipo de programa pode ser encontrado facilmente na Internet. Através do programa, é possível criar senhas mais difíceis de serem quebradas, pois ele gera uma combinação aleatória de caracteres sem nenhum significado.

Além de utilizar senhas mais seguras, é importante trocar as senhas com freqüência. Isto é necessário porque alguém já pode ter descoberto uma senha, ou pode estar tentando descobrir. Conseqüentemente, o segundo passo foi a preparação dos sistemas para expiração automática das senhas num período de dois meses, mesmo assim os funcionários foram educados a fazer esse procedimento manualmente, pois muitos do serviços disponibilizados na rede não possuem essa funcionalidade.

3.4.6. Centralização e Auditoria dos Registros (Logs)

Por padrão os logs são armazenados localmente em cada equipamento, muitas vezes o sistema nem mesmo está configurado para gerar as mensagens de log.

Os logs distribuídos em várias máquinas podem tornar o trabalho de auditoria dos registros complicado, além disso, se um equipamento for comprometido os seus registros podem ser excluídos pelo invasor.

O ideal é manter um servidor somente com a função de armazenar os logs de todos os equipamentos, criando uma estrutura centralizada. Aumentando a segurança e facilitando o trabalho de verificação.

Seguindo essa linha de raciocínio, foi adicionado um novo servidor com a função específica de centralizar os logs. Esse novo servidor utiliza um programa chamado SyslogNG, que é compatível com o padrão Syslog[6] do Unix, Tal programa permite uma maior filtragem das informações quando comparado com o SysLog original do Linux.
Todos servidores, e os equipamentos que possuem o serviço de log, foram configurados para enviar as suas mensagens ao servidor de logs ao invés de mantê-las localmente. Por sua vez o servidor de logs filtra essas mensagens e as armazena de acordo com a sua classificação, facilitando o trabalho de auditoria.

---

[6] SYSLOG é o padrão UNIX para armazenamento e comunicação local ou remota de mensagens de log. Geralmente um processo chamado syslogd é iniciado junto a inicialização de sistemas operacionais derivados do Unix, esse processo recebe as mensagens provenientes de outros programas executados na máquina e as armazena localmente ou em um servidor syslog. Muitos equipamentos de rede, como roteadores e servidores de acesso remoto, possuem a funcionalidade do syslog.

Também foram utilizadas algumas ferramentas, além de scripts desenvolvidos internamente, que automatizam a verificação e o alerta de possíveis tentativas de invasão ou acesso irregular ao sistema. Mesmo assim, semanalmente os logs são verificados de forma manual pela equipe de administração de sistemas, a fim de não deixar escapar nenhum registro.

3.4.7. Criptografia para Proteção dos Dados

3.4.7.1. VPNs entre os servidores

Os equipamentos dentro do segmento de Servidores precisam se comunicar para troca de informações sobre autenticação de usuários, consultas no banco de dados e para envio das mensagens para o servidor de logs. A maioria dessa comunicação trafega sem criptografia, dessa forma se um invasor comprometer alguma máquina do segmento ele poderá monitorar o tráfego. Mesmo que este segmento esteja utilizando um Switch para maior proteção contra Sniffers, existem formas de ataque que fazem com que o Switch se comporte como um HUB.

Para proteger os dados trafegados e garantir a confiabilidade foram implementadas VPNs entre os servidores que necessitam de comunicação. O programa utilizado foi o VTUN, ele utiliza o algoritmo de criptografia Blowfish que é leve ao mesmo tempo sem perder a segurança. A configuração do programa é muito simples, depois de estar funcionando ele cria interfaces de rede virtuais nas quais todo os dados trafegados são criptografados.

A utilização das VPNs não teve grandes reflexos na performance da rede, não chegou a afetar a execução de nenhum serviço, trouxe apenas a vantagem de estar tornando a comunicação entre os servidores ainda mais segura.

3.4.7.2. Criptografia para o comércio eletrônico

Essa foi uma das fases mais importantes do desenvolvimento prático do estágio, e contempla a aplicação direta de recursos para proteção das transações de comércio eletrônico do sistema.

Como descrito no capítulo 3.4.4, foi designado um novo servidor específico para dar suporte ao sistema de comércio eletrônico. Para proteção das transações realizadas através da Internet, ou seja, a confiabilidade e integridade dos dados trafegados através da conexão

entre os clientes das lojas virtuais e o sistema, foi utilizado o protocolo de criptografia SSLv2 através do programa ModSSL. Esse programa atua como um módulo que é agregado junto ao servidor WEB Apache, que é o servidor WEB utilizado pela empresa.

Para o correto funcionamento do SSL é necessária a utilização de um certificado digital fornecido por alguma autoridade certificadora reconhecida, esse certificado garante a identidade do servidor aos clientes. Sem o certificado, a comunicação SSL pode até ser estabelecida, mas o navegador web do usuário/cliente vai emitir um alerta informando que a identidade desse servidor não pode ser verificada.

Sendo assim, a compra do certificado de 128 bits foi efetuada junto a uma empresa Americana chamada Thawte (http://www.thawte.com). Apesar de existir uma empresa brasileira capacitada a fornecer certificados nesse nível de segurança (128bits), o custo da empresa estrangeira era bem mais baixo.

A utilização do SSL com o certificado de 128bits pode garantir a segurança dos dados trafegados através da Internet, assim protegendo informações importantes como números de cartão de crédito e dados particulares dos clientes. Mesmo assim o processo ainda não estava completo, era necessário garantir a segurança dos dados também ao serem enviados pelo sistema de comércio eletrônico aos administradores das lojas virtuais. Optou-se por não armazenar nenhum dado importante, como números de cartão de crédito, no banco de dados do servidor de comércio eletrônico. Assim que os pedidos são efetuados esses dados são criptografados, através do software GnuPG, e enviados diretamente aos lojistas, onde a transação de compra é finalizada. Para assegurar esse novo envio de dados foi utilizada criptografia assimétrica com chaves de 4096bits. Para cada nova loja virtual implantada é criado um par de chaves que é instalado no computador localizado no estabelecimento físico do cliente, responsável por receber os pedidos provenientes do sistema de comércio eletrônico. No servidor ficam localizadas as chaves públicas das lojas virtuais, quando o pedido é efetuado, os dados são criptografados e enviados aos lojistas.

Todo esse processo poderia ser facilitado e ainda se tornar mais seguro se fosse utilizada a tecnologia SET. Nesse caso nem mesmo os lojistas teriam acesso aos números dos cartões de crédito dos clientes, esses números seriam enviados diretamente para operadora de cartão de crédito que autorizaria o compra e transferiria os fundos eletronicamente para a loja. Entretanto depois de diversos contatos sem sucesso junto a VisaNET e Globalis, empresas responsáveis pela implantação do SET no Brasil, pudemos verificar que as ferramentas para utilização desse protocolo não estão disponíveis para o sistema operacional Linux, somente para Microsoft Windows NT/2000 ou o Unix Solaris da Sun Microsystems. Além disso, a utilização do SET envolveria mais custos para as lojas virtuais, tornando ainda mais difícil a aceitação dessa tecnologia.

Mesmo sem a utilização do SET, através das tecnologias aplicadas foi possível garantir um nível elevado de segurança, onde somente os lojistas têm acesso aos dados de seus clientes, garantindo uma relação de confiança equivalente ao das compras convencionais. Caso o servidor viesse a ser comprometido, nenhum dado importante sobre os clientes estaria disponível no banco de dados, diminuindo consideravelmente as conseqüências de um ataque.

3.4.7.3. Armazenamento dos Backups

Os backups estavam sendo feitos de maneira correta, garantindo que a informação estivesse disponível para recuperação no caso de um problema. Eles armazenam dados importantes de todos os servidores, como configurações, listas de usuários e outros tipos de dados. Caso uma cópia desses backups pudesse ser obtida por alguém mal intencionado, toda a empresa pode ficar comprometida.

Dessa maneira, para proteção dos backups foi aplicada a criptografia assimétrica utilizando o programa GNUPG. Foram criados dois pares de chaves de 4096 bits, um par contendo a chave pública e privada dos servidores, e outro par contendo as chaves do grupo de administradores de sistemas. Sempre que as cópias eram geradas nos servidores, elas eram automaticamente criptografadas utilizando a chave pública da equipe de administração de sistemas, além disso, as cópias eram assinadas digitalmente com a chave privada dos servidores. Assim somente os administradores de sistemas, de posse da sua chave privada, podem decriptar os dados armazenados nos backups, e ainda confirmar a sua origem e integridade comparando a assinatura digital com a chave pública dos servidores.

Com a proteção dos backups, mesmo que a cópia levada semanalmente por um dos sócios da empresa fosse roubada, as informações contidas nela estariam seguras. Além disso, somente os funcionários autorizados têm acesso aos dados do backup, pois apenas eles têm acesso à chave privada necessária para acessar os dados.

3.4.7.4. Gerenciamento dos Servidores

A equipe de administração de sistema necessita constantemente acessar remotamente os servidores para manutenção e implementação de novas tecnologias. Para possibilitar essa tarefa foi utilizado o protocolo SSH (Secure Shell) através do programa OpenSSH. Esse programa torna possível o acesso remoto ao shell[7] dos servidores de forma segura, ele criptografa todo o tráfego da transmissão, impedindo que possam ser capturados comandos ou senhas. O programa ainda permite a autenticação dos usuários através de chaves de criptografia assimétrica. Sendo assim, para autenticação foi criado um par de chaves para cada um dos administradores de sistemas, as suas chaves públicas foram instaladas nos servidores, e as privadas em suas estações. Dessa forma, o acesso é permitido somente aos administradores de posse da sua chave privada. O uso da criptografia assimétrica para autenticação permite uma segurança incomparável com a utilização de senhas, pois ela elimina a possibilidade de quebra desse controle através de Força-Bruta ou Ataque de dicionário.

3.4.8. Auditoria no código fonte do sistema de comércio eletrônico

Mesmo se o servidor que dá suporte ao comércio eletrônico fosse devidamente protegido, falhas no sistema desenvolvido pela Empresa poderiam criar novas vulnerabilidades. Por isso, a fase de auditoria no código fonte teve grande importância.

Seguindo as recomendações expostas na fundamentação teórica, as seguintes ações foram realizadas com objetivo de assegurar o sistema:

- Foram removidas todas as chamadas de programas executáveis do sistema operacional. Essas funções foram desenvolvidas internamente ao programa utilizando as funções disponíveis da linguagem. Assim o sistema não fica vulnerável a falhas de outros programas.
- Foram verificadas todas as funções que recebiam entradas de dados provenientes dos usuários através da Internet. Assim foram criadas rotinas que validam esses dados antes de qualquer outra ação.

---

[7] Shell é nome designado ao prompt de comandos dos ambientes UNIX. Geralmente para acessar o Shell remotamente é utilizado o protocolo TELNET, esse protocolo é muito falho na questão da segurança porque os dados trafegados através dele e o seu processo de autenticação não utilizam criptografia.

- Foi dada uma atenção especial a todas as funções que poderiam gerar mensagens de erro. Essas mensagens foram traduzidas para uma forma mais simples e informações adicionais que poderiam fornecer informações valiosas aos invasores foram removidas.
- A linguagem PHP, que processa os códigos fontes do sistema, foi atualizada para sua última versão. Ela também foi incluída no processo de atualização realizado pelos administradores de sistemas. Além disso, ela foi configurada utilizando os seus recursos de restrição de acesso e segurança.
- Todas a senhas de acesso ao banco de dados e outros recursos foram armazenadas em diretório protegido no servidor WEB, restringindo o seu acesso somente ao sistema.

Através dessas ações, e posteriormente o uso de criptografia, várias vulnerabilidades antes não identificadas foram corrigidas e a segurança do sistema foi elevada.

3.4.9. Proteção Contra Malware

A proteção contra vírus e outras pragas virtuais é um ponto muito importante na segurança de uma organização. Esses programas maliciosos podem fazer grandes estragos, muitas vezes irreversíveis. É necessário que sejam tomadas medidas para evitar a ação dessas pragas.

As estações já utilizavam o programa comercial de Antivírus AVP, sendo que a sua base de dados de informações sobre vírus era freqüentemente atualizada. Entretanto os servidores não estavam devidamente protegidos.

Há algum tempo atrás era difícil ou praticamente inexistente a possibilidade do Linux ser infectado por algum tipo vírus. Devido à maioria dos seus programas serem de código aberto (Open Source), é possível fazer uma verificação que busque códigos maliciosos em um programa. Entretanto atualmente muitos pacotes de programas são distribuídos em forma binária, ou seja, os programas já estão compilados para facilitar a instalação por parte dos usuários. Dessa forma, esses programas previamente compilados podem conter códigos de vírus ou outras pragas. Além disso, os Worms mais modernos se espalham através de brechas em diversos sistemas operacionais, aumentando ainda mais a necessidade de utilização de um programa de antivírus.

Sendo assim, para proteção dos servidores foi instalado o Antivírus AVP – Versão Linux. O programa fica residente em memória a procura pela execução de qualquer código malicioso conhecido, ainda é possível fazer a verificação manual de vírus nos arquivos do

sistema. O programa ainda permite a atualização da sua base de reconhecimento de vírus seja feita através da Internet, de forma automática.

Além da proteção fornecida pelo antivírus, foi definido que se daria preferência aos programas distribuídos em forma de código fonte de origem devidamente verificada, assim dificultando que códigos maliciosos venham agregados a programas binários previamente compilados.

3.4.10. Instalação dos Sistemas de Identificação de Intrusão

3.4.10.1. – NIDS

Para identificação de intrusão através de rede foram utilizados dois programas descritos a seguir:

- SNORT: É um sistema capaz de analisar o tráfego da rede em tempo real. Baseia-se em uma base de dados para identificar os ataques. Ele usa uma linguagem flexível para determinação das regras que descrevem o tráfego que deve ser analisado ou ignorado, como também oferece um mecanismo de detecção que utiliza uma arquitetura modular através de plugins. O programa também tem potencialidade de gerar alertas em tempo real através do envio de mensagens ao syslog, alertas em arquivo, ou outros meios.
- NESSUS: Ao contrário do Snort que somente monitora e alerta as tentativas de invasão, o Nessus identifica as vulnerabilidades dos sistemas através da rede. Ao invés de monitorar o tráfego, ele realiza a verificação de segurança num sistema somente quando solicitado. O seu funcionamento é baseado em um conjunto de regras que definem ações a serem realizadas para identificar as vulnerabilidades. Ele utiliza uma arquitetura cliente-servidor, onde o servidor realiza os testes e o cliente apenas comanda as ações e recebe os resultados.

Apesar de ambos serem considerados IDS de rede, os sistemas não se excluem. O Snort é capaz de identificar e alertar os ataques durante a sua execução, enquanto o Nessus permite realizar uma busca de vulnerabilidades nos hosts da rede.

No ambiente empresa foram implementadas as duas ferramentas diretamente no firewall. Somente o firewall pode monitorar todos os dados trafegados na rede, necessário para o Snort; e somente ele tem acesso sem restrições a todos segmentos de rede, necessário para o módulo servidor do Nessus.

Ambas as ferramentas possuem mecanismos de atualização automática da sua base de dados que foram devidamente configurados para serem executados diariamente. Além disso, como o Nessus requer a operação manual do seu modo cliente para realização das verificações, foi determinado que a cada dois dias seria realizada uma verificação utilizando o Nessus.

Dependendo do nível de reconhecimento selecionado no Snort, ele pode gerar um grande número de mensagens de alerta, dificultado o trabalho de reconhecimento do ataque. Para facilitar o entendimento das mensagens geradas pelo Snort foram utilizados alguns scripts que lêem os arquivos de log gerados pelos sistemas e extraem as informações mais importantes.

A utilização dessas duas ferramentas forneceu informações importantes para a segurança da organização. Logo de início o Nessus apontou vulnerabilidades antes desconhecidas que foram imediatamente corrigidas, e agora o Snort pode fornecer informações sobre o que está acontecendo na rede, identificando tentativas de ataques e possibilitando a execução de medidas de reação.

3.4.10.1. – HIDS

A ferramenta utilizada na detecção de intrusão de hosts foi o Tripwire. Essa ferramenta verifica quais foram as mudanças realizadas no sistema. O programa monitora os atributos dos arquivos que não devem ser mudados, incluindo assinaturas binárias, tamanho, permissões, etc. Inicialmente o programa é configurado para definição de quais arquivos devem ser monitorados e quais são as mudanças aceitáveis que podem ocorrer com eles. Então o programa gera um banco de dados criptografado com o estado atual de todos esses arquivos, posteriormente é possível fazer uma verificação comparando-se os arquivos com os dados do banco de dados, alertando quais atributos dos arquivos foram modificados fora do padrão.

No ambiente da Empresa, o programa foi configurado para fazer verificações diárias dos arquivos em cada servidor, além disso, a cada dois dias a base de dados é atualizada a fim de manter as informações atualizadas sobre os arquivos.

A parte mais difícil de implementação desse programa é a sua configuração inicial, dependendo o número dos arquivos monitorados e seus atributos, o número de falsos alertas pode ser grande até se ter uma configuração realmente funcional. Nesse momento muitos administradores de sistemas acabam por desistir de utilizá-lo.

Apesar da dificuldade da instalação, o Tripwire é uma ferramenta extremamente útil que pode detalhar todas as mudanças ocorridas nos arquivos do sistema, permitindo identificar todas as ações realizadas por um hacker no caso de uma invasão.

3.4.11. Segurança Física

Os servidores estavam agrupados em uma sala onde o acesso não era controlado, não havia regras que definissem quais pessoas tinham acesso a esse local. Esse fato era muito grave e poderia pôr fim em todo o projeto lógico de segurança. Para solucionar esse problema foram definidas regras de quais pessoas teriam acesso à sala de servidores, inicialmente somente os administradores de sistemas. Além disso, para garantir a segurança física dos equipamentos contra roubo, foi instalado mais um ponto de alarme nesse local.

Para garantia da disponibilidade, foram revisadas todas as instalações elétricas e um ar condicionado foi instalado unicamente para manter a temperatura da sala.

Mesmo sendo ações simples, elas são fundamentais para a segurança da empresa. Sem uma garantia mínima da segurança física dos equipamentos, qualquer projeto de segurança pode ser anulado.

3.4.12. Ataques Internos e Engenharia Social

Apesar da segurança contra ataques internos ser um fator muito importante, no ambiente dessa Empresa ela não representa um grande risco, por se tratar de uma empresa de poucos funcionários. Mesmo assim esse ponto não pode deixar de ser considerado, pois a Engenharia Social poderia ser utilizada para obtenção de informações. Dessa forma houve um processo de educação dos funcionários no qual foram determinadas as suas responsabilidades para manutenção da segurança da informação, além de serem definidas quais informações são sigilosas e de propriedade da empresa.

Num âmbito mais técnico, a utilização do firewall para controle do tráfego, o SSH para gerenciamento dos servidores, e os sistemas de IDS possibilitaram um maior controle dos acessos internos e a identificação de possíveis ataques.

3.4.13. Plano de Resposta a Incidentes

Como um dos objetivos principais da realização do trabalho, o plano de resposta a incidentes não poderia deixar de constar nas atividades práticas. Entretanto o conteúdo desse plano não pode ser exposto no trabalho devido a restrições impostas pela empresa. Nesse documento constam informações sigilosas sobre as pessoas responsáveis e os procedimentos que devem ser adotados no caso de incidentes envolvendo a segurança das informações.

3.7. Ações Futuras

Apesar da política da segurança ser um ponto muito importante em qualquer trabalho envolvendo segurança da informação, e devido a essa importância ter sido tratada na fundamentação teórica, não houve tempo suficiente dentro da realização do estágio para o seu desenvolvimento. Ainda assim, a política da segurança, bem como outros pontos serão considerados em ações futuras, além do estágio, a serem executadas na empresa. Podemos destacar:

- Implementação de Cluster[8] para o servidor de Comércio Eletrônico, a fim de garantir maior disponibilidade;
- Testar o uso de outros sistemas operacionais como FreeBSD e OpenBSD, e suas ferramentas de segurança;
- Realização de testes de penetração para comprovar a validade das medidas e ferramentas de segurança aplicadas;

[8] Clusters são servidores que atuam como backup de outros equipamentos para o caso de falha, podendo assumir o papel do equipamento com falha em tempo real. O termo também pode ser utilizado para servidores que trabalham em paralelo com a função de aumentar o poder de processamento.

CONCLUSÃO

O trabalho de estágio relacionado à segurança da informação envolveu a aplicação de conhecimentos de diversas outras áreas da informática. Nesse aspecto foram de grande valia as horas despendidas no processo de estudo das tecnologias a serem aplicadas e os conhecimentos obtidos através da Universidade. Foram aplicados conceitos relacionados às disciplinas de Linguagens e Técnicas de Programação, Comunicação de Dados e Sistemas Operacionais.

Como resultado, o estudo e aplicação dos conceitos expostos puderam ser concretizados em ações que trouxeram grandes benefícios para empresa onde o estágio foi realizado. Todos os objetivos iniciais foram atendidos, a eliminação das vulnerabilidades encontradas na empresa fortaleceu todos os elos que compõem segurança da organização, enquanto a aplicação de novas medidas e ferramentas de segurança criou um ambiente mais fácil de ser controlado e monitorado. As principais ameaças agora podem ser medidas, os ataques identificados, e as ações de resposta estão bem definidas e documentadas. Todos esses benefícios puderam criar um ambiente adequado para os novos serviços lançados pela empresa, como o comércio eletrônico, além de aumentar a segurança da organização como um todo.

Não desmerecendo os benefícios obtidos, alguns problemas foram criados junto a essa nova realidade: a dificuldade de implementação de novos serviços e equipamentos devido ao grande número de regras de controle, e o excesso de informações e alertas gerados pelos sistemas de segurança que acabam por ocupar muito o trabalho dos administradores de sistemas.

Ao término das atividades, é gratificante constatar os bons resultados obtidos. Entretanto o trabalho não se encerra por aqui. Novas falhas e vulnerabilidade em sistemas são descobertas diariamente, os invasores possuem ferramentas cada vez mais automatizadas, e conforme o ambiente cresce, torna-se mais difícil controlá-lo. Sendo assim, pode-se concluir que segurança da informação deve ser um processo contínuo que faça parte das atividades da empresa, sempre objetivando atender os seus princípios básicos: Confiabilidade, Autenticidade, Integridade e a Disponibilidade.

BIBLIOGRAFIA

1. ALBERTIN, Alberto Luiz. **Comércio Eletrônico.** 2. ed. São Paulo: Atlas, 2000.

2. ALEGRE, Liliana Esther Velásquez. **Os Logs como Ferramenta de Detecção de Intrusão,** obtido através da Internet. http://www.rnp.br/newsgen/9905/logs.shtml, maio 1999.

3. ANONYMOUS. **Maximum Linux Security.** Estados Unidos – Indianapolis: Sams, 1999.

4. BACE, Rebecca. **NIST Special Publication on Intrusion Detection Systems**, obtido através da Internet. http://www.nist.gov. 09 abr. 2001.

5. CAMEPELLO, Rafael et al. **Anais do WSEG'2001: Workshop em Segurança de Sistemas Computacionais 2001.** Porto Alegre: SBC, 2001.

6. CERT Coordination Center, http://www.cert.org

7. CLIFF, A. **Password Crackers – Ensuring the Security of Your Password,** obtido através da Internet. http://www.securityfocus.com/, 09 abr. 2001.

8. ED. Consultoria. **Criptografia,** obtido através da Internet. http://www.edconsultoria.com.br, 25 fev. 2001

9. ED. Consultoria. **Estudo de Vírus,** obtido através da Internet. http://www.edconsultoria.com.br, 25 fev. 2001

10. FONTES, Edison. **Política da Segurança da Informação,** obtido através da Internet. http://www.modulo.com.br/, 03 nov. 2000.

11. FYODOR. **NMAP – The Network Mapper,** obtido através da Internet. http://www.insecure.org/nmap, 10 mar. 2001.

12. **Guia Internet de Conectividade.** 2. ed. São Paulo: Cyclades Brasil, 1999.

13. HAICAL, Cristiani. **Malware,** obtido através da Internet. http://www.modulo.com.br/, 01 mar. 2001.

14. HAZARI, Sunil. **Firewalls for Beginners,** obtido através da Internet. http://www.securityfocus.com/, 06 nov. 2000.

15. LIMA, Marcelo B. Firewalls – Uma Introdução à Segurança. **Revista do Linux.** Curitba, n.2, p. 16, fev. 2000.

16. Linux Security, http://www.linuxsecurity.com.br

17. JOHNSON, John D. **Is It Safe to Go Outside Without Backup?,** obtido através da Internet. http://www.securityportal.com, 01 nov. 2000.

18. Modulo e-security, http://www.modulo.com.br

19. Packet Storm, http://packetstorm.securify.com/

20. PANETTA, Nelson. Criptografia. **Security Magazine.** São Paulo, n.6, p. 10-16, ago. 2000.

21. PANETTA, Nelson. Criptografia. **Security Magazine.** São Paulo, n.7, p. 8-14, out. 2000.

22. PANETTA, Nelson. Criptografia. **Security Magazine.** São Paulo, n.8, p. 10-16, dez. 2000.

23. PETEANU, Razvan. **Best Practices for Secure Web Development: Technical Details**. obtido através da Internet. http://www.securityportal.com, 10 nov. 2000.

24. PUTTINI, Ricardo S.; SOUZA, Rafael T. de. **Principais Aspectos da Seguraça,** obtido através da Internet. http://webserver.redes.unb.br/security/introducao/aspectos.html, fev. 2001.

25. **Raid.edu**. AC&NC – Advance Computer & Networks Corporation. obtido através da Internet. http:// www.acnc.com. 8 abr. 2001

26. Sans Institute, http://www.sans.org

27. SecureNET, http://www.securenet.com.br

28. Security Portal: http://www.securityportal.com

29. Secure Eletronic Transation: http://www.setco.org

29. TIMS, Rick. **Social Engineering: Policies and Education a Must,** obtido através da Internet. http://www.sans.org/, 16 fev. 2001.